Military EMBEDDED SYSTEMS

@military_cots

MIL-EMBEDDED.COM

April/May 2017 | Volume 13 | Number 3

UNMANNED UNDERSEA VEHICLES EVOLVING QUICKLY

P 20

UNMANNED SYSTEMS ISSUE

P 26

The commonality of COTS solutions for UUVs and UAVs
By Mike Southworth, Curtiss-Wright Defense Solutions

RF & microwave technology enabling multimission unmanned systems

P 30

Volume 13
Number 3

April/May 2017

Military EMBEDDED SYSTEMS

www.mil-embedded.com


20


26


30


38


34

WEB RESOURCES

Subscribe to the magazine or E-letter
Live industry news | Submit new products
http://submit.opensystemsmedia.com

White papers:
Read: http://whitepapers.opensystemsmedia.com
Submit: http://submit.opensystemsmedia.com

www.linkedin.com/groups/Military-Embedded-Systems-1864255

@military_cots

Published by: OpenSystems media

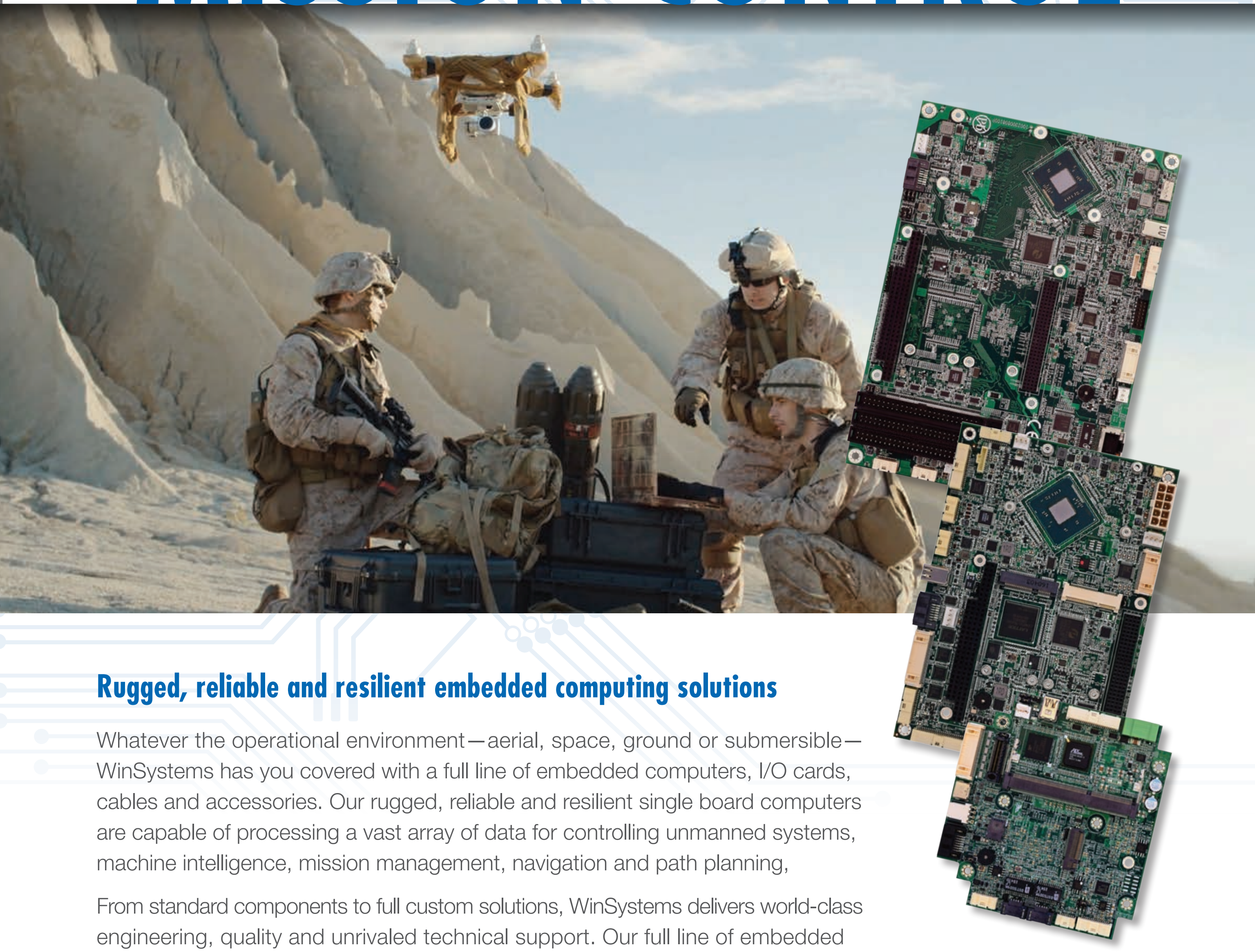
ON THE COVER:

Top image:
Lockheed Martin's Marlin unmanned undersea vehicle can carry out a variety of military and commercial missions. Image courtesy of Lockheed Martin.

Bottom image:
An RQ-4 Global Hawk unmanned aerial system (UAS) soars through the sky to record intelligence, surveillance, and reconnaissance data. Air Force courtesy photo.

ISSN: Print 1557-3222

MISSION CONTROL



Rugged, reliable and resilient embedded computing solutions

Whatever the operational environment—aerial, space, ground or submersible—WinSystems has you covered with a full line of embedded computers, I/O cards, cables and accessories. Our rugged, reliable and resilient single board computers are capable of processing a vast array of data for controlling unmanned systems, machine intelligence, mission management, navigation and path planning,

From standard components to full custom solutions, WinSystems delivers world-class engineering, quality and unrivaled technical support. Our full line of embedded computers, I/O cards, and accessories help you design smarter projects offering faster time to market, improved reliability, durability and longer product life cycles.

Embed success in every application with ***The Embedded Systems Authority!***

EBC-C413
EBX-compatible SBC with Latest Generation Intel® Atom™ E3800 Series Processor

EPX-C414
Quad-Core Freescale i.MX 6Q Cortex A9 Industrial ARM® SBC

PX1-C415
PC/104 Form Factor SBC with PCIe/104™ OneBank™ expansion and latest generation Intel® Atom™ E3900 Series processor

SCADA | ENERGY | IOT | AUTOMATION | TRANSPORTATION

Single Board Computers | COM Express Solutions | Power Supplies | I/O Modules | Panel PCs

WinSystems®
The Embedded Systems Authority

817-274-7553 | www.winsystems.com
ASK ABOUT OUR PRODUCT EVALUATION!
715 Stadium Drive, Arlington, Texas 76011

intel IoT Solutions Alliance

QUALITY ISO 9001:2008 CERTIFIED

ADVERTISER INFORMATION

EVENTS

IMS 2017 – IEEE International Microwave Symposium
June 4-9, 2017 • Honolulu, HI
www.ims2017.org

MilSatCom USA
June 28-29, 2017 • Arlington, VA
www.smi-online.co.uk/defence/northamerica/MilSatCom-USA

Military EMBEDDED SYSTEMS

GROUP EDITORIAL DIRECTOR John McHale jmchale@opensystemsmedia.com
ASSISTANT MANAGING EDITOR Lisa Daigle ldaigle@opensystemsmedia.com
SENIOR EDITOR Sally Cole scole@opensystemsmedia.com
ASSOCIATE EDITOR Mariana Iriarte miriarte@opensystemsmedia.com
DIRECTOR OF E-CAST LEAD GENERATION AND AUDIENCE ENGAGEMENT Joy Gilmore jgilmore@opensystemsmedia.com
CREATIVE DIRECTOR Steph Sweet ssweet@opensystemsmedia.com
SENIOR WEB DEVELOPER Konrad Witte kwitte@opensystemsmedia.com
WEB DEVELOPER Paul Nelson pnelson@opensystemsmedia.com
DIGITAL MEDIA MANAGER Rachel Wallace rwallace@opensystemsmedia.com
CONTRIBUTING DESIGNER Joann Toth jtoth@opensystemsmedia.com

VITA EDITORIAL DIRECTOR Jerry Gipper jgipper@opensystemsmedia.com

SALES

SALES MANAGER Tom Varcie tvarcie@opensystemsmedia.com (586) 415-6500
MARKETING MANAGER Eric Henry ehenry@opensystemsmedia.com (541) 760-5361
STRATEGIC ACCOUNT MANAGER Rebecca Barker rbarker@opensystemsmedia.com (281) 724-8021
STRATEGIC ACCOUNT MANAGER Bill Barron bbarron@opensystemsmedia.com (516) 376-9838
STRATEGIC ACCOUNT MANAGER Kathleen Wackowski kwackowski@opensystemsmedia.com (978) 888-7367
SOUTHERN CAL REGIONAL SALES MANAGER Len Pettek lpettek@opensystemsmedia.com (805) 231-9582
SOUTHWEST REGIONAL SALES MANAGER Barbara Quinlan bquinlan@opensystemsmedia.com (480) 236-8818
NORTHERN CAL STRATEGIC ACCOUNT MANAGER Sean Raman sraman@opensystemsmedia.com (510) 378-8288
ASIA-PACIFIC SALES ACCOUNT MANAGER Elvi Lee elvi@aceforum.com.tw
BUSINESS DEVELOPMENT EUROPE Rory Dear rdear@opensystemsmedia.com +44 (0)7921337498

OpenSystems media®
WWW.OPENSYSTEMSMEDIA.COM

PRESIDENT Patrick Hopper phopper@opensystemsmedia.com
EXECUTIVE VICE PRESIDENT John McHale jmchale@opensystemsmedia.com
EXECUTIVE VICE PRESIDENT Rich Nass rnass@opensystemsmedia.com
CHIEF FINANCIAL OFFICER Rosemary Kristoff rkristoff@opensystemsmedia.com
CHIEF TECHNICAL OFFICER Wayne Kristoff
EMBEDDED COMPUTING BRAND DIRECTOR Rich Nass rnass@opensystemsmedia.com
EMBEDDED COMPUTING EDITORIAL DIRECTOR Curt Schwaderer cschwaderer@opensystemsmedia.com
TECHNOLOGY EDITOR Brandon Lewis blewis@opensystemsmedia.com
CONTENT ASSISTANT Jamie Leland jleland@opensystemsmedia.com
CREATIVE PROJECTS Chris Rassiccia crassiccia@opensystemsmedia.com
FINANCIAL ASSISTANT Emily Verhoeks everhoeks@opensystemsmedia.com
SUBSCRIPTION MANAGER subscriptions@opensystemsmedia.com

CORPORATE OFFICE
16626 E. Avenue of the Fountains, Ste. 201 • Fountain Hills, AZ 85268 • Tel: (480) 967-5581

REPRINTS

WRIGHT'S MEDIA REPRINT COORDINATOR Wyndell Hamilton whamilton@wrightsmedia.com (281) 419-5725

Economics of modularity and reuse, continued

By John McHale, Editorial Director

In our March issue, I talked about how electronics-reuse initiatives within the Department of Defense (DoD) such as Hardware Open Systems Technology (HOST), the Sensor Open Systems Architecture (SOSA), and the Future Airborne Capability Environment (FACE) are driving commonality in avionics, radar, unmanned systems, and other defense applications, thus enabling long-term cost savings in an era of expensive platforms such as the F-35 Joint Strike Fighter.

The discussion continued in our monthly COTS Confidential roundtable article, titled "Trump defense budget increase, open architectures, and export reform" (http://bitly.com/2oFrrka) in the McHale Report newsletter. The upshot: While all agree on the economic and operational benefits such initiatives bring, not everyone believes the services will work well enough together to get the most out of the various efforts.

"Standards like FACE, SOSA, and OMS [Open Mission Systems] will drive far greater levels of interoperability and allow systems deployed today to constantly upgrade their competitive edge for many years to come," says Chip Downing, Senior Director, Business Development, Aerospace & Defense at Wind River Systems. "Static, proprietary systems of the past will have to open up to maintain their relevance to future missions."

Modularity is the key, as it solves not only cost but also integration and maintenance issues over the long term.

"Modularity makes configurability, maintenance, and upgrades much faster, easier, and cheaper," says Ray Alderman, Chairman of the Board of VITA, in the COTS Confidential article. "It's not just about designing chips and algorithms; it's how we put them together. We need to be in a position to have modularity in hardware and software to do upgrades on the fly, which will save time and money. Modularity does that."

Major programs in the Air Force, Navy, and Army are now focused on increased modularity in electronic systems: The Air Force has OpenPod, the Navy has OpenBay, while the Army has OpenRack, he continues. "How far each of these programs will go is questionable. But, with defense spending under pressure to be more cost-effective, they could each enjoy some level of popularity. We need to use the money we have more efficiently and these modularity programs are a move in that direction."

The commercial world has already embraced open architectures en masse; these days, the military follows the commercial world on technology developments. The trend toward open architectures is "unquestionably here to stay, both in defense and commercial industries," says Manuel Uhm, Director of Marketing, Ettus Research, a National Instruments company and Chair of the Board of Directors of the Wireless Innovation Forum in the article. "In the defense space, there is a huge benefit in terms of broadening the ecosystem, increasing competition, avoiding vendor lock-in, and ensuring security through source-code traceability.

"Static, proprietary systems of the past will have to open up to maintain their relevance to future missions," says Chip Downing at Wind River Systems.

"Several commercial industries have also firmly embraced open architectures and open standards," Uhm continues. "Linux may have kicked off this trend in a big way, but in the telecommunications space, the advent of software-defined networking has led to an explosion in support for open source and open standards, such as OpenFlow, OpenDaylight, and OpenStack."

Playing together in the same reuse sandbox

"Could all the services work together, under a collective open architecture program, to share commonly needed modules like CPUs or communications interfaces or sensors across different platforms?" Alderman asks. "Maybe that's what could happen with the HOST and SOSA activities, but I doubt it. They might if they continue to move toward a cross-domain strategy, which roughly means leveraging resources across multiple services and warfare domains. For example, if a Navy resource is at sea and needs to destroy a target offshore, it calls the Army or Air Force to take out the target. This cross-domain concept could be the catalyst to force the services to come up with more standards for common electronics."

I'm more hopeful they will actually work together, mostly due to the fact that they really have no choice. Doing things the old way with legacy and proprietary systems, with the government funding technology development from the ground up, is unfair to the taxpayer and the warfighter and – as I said in my March column – just plain economically unsound.

One of the lead minds behind SOSA has a similar view in the Executive Outlook on page 16 in this issue: "The DoD and government community realizes that current and future systems are growing in complexity," says Dr. Ilya Lipkin, Lead Manager for SOSA at the U.S. Air Force Life Cycle Management Center. "Disparate groups and entities have seen, independently, the benefit of moving to a modular open architecture environment for a wide variety of applications. There is a convergence of applications that are data and information driven. This, in turn, drives commonality across hardware and software modules."

Electronic warfare and FPGAs: The need for speed

By Charlotte Adams

An Abaco Systems perspective on embedded military electronics trends

Electronic warfare (EW), the use of the electromagnetic spectrum to foil enemy forces and protect friendly ones, is perhaps the most time-sensitive of all the weapons in the military arsenal: a matter of nanoseconds could make the difference between life and death. That's why latency is so critical to EW processing systems. If a radar-guided missile is heading for your aircraft at Mach 5, the aircraft's radar jammer had better be quick – quick to take in the signal, manipulate it, and retransmit it to fool the adversary with false targets or misleading data on size, distance, heading, speed. Digital RF memories (DRFMs), the specialized RF jammers that do just that, require receive-response latencies of 20 to 100 nanoseconds. Compared to radars – which transmit pulses and receive echoes – DRFMs – which receive pulses and retransmit the signals modulated with jamming techniques – have much more stringent latency requirements.

Survival isn't getting any easier, as adversaries deploy advanced weaponry on the electronic battlefield. The bandwidth of the analog signals that are being received by EW systems is expanding, while higher data volumes are coming in on a larger number of channels.

The need for EW speed – never more urgent than now – is driving the incorporation of computationally intensive field-programmable gate arrays (FPGAs), as well as faster data conversion chips, into front-end EW processing systems.

Fortunately, the commercial off-the-shelf (COTS) parts industry is keeping up in both areas. In recent years, for example, FPGAs have approximately doubled the density of their processing resources while cutting power consumption in half.

The latest devices come in multiple flavors. Some FPGAs feature millions of configurable logic blocks – flexible math operators – giving them massive computational power. Other FPGAs encompass both configurable logic blocks and embedded general-purpose processors (GPPs). In EW applications, the GPP elements of these hybrid chips

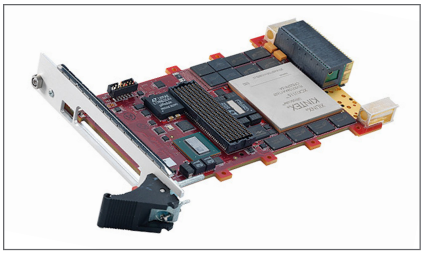


Figure 1 | The Abaco Systems VP880 3U VPX FMC+ carrier card features Xilinx's latest UltraScale FPGA and FPGA-hybrid Zynq UltraScale technology.

can be used for monitoring applications or for updating target profiles.

Industry watchers predict that future FPGAs will even incorporate analog-to-digital converters (ADCs) and digital-to-analog converters (DACs), further decreasing end-to-end processing latencies.

Boards shrink

While FPGAs are growing larger and denser, their carrier boards are getting smaller. Multiple FPGAs, along with ADCs, DACs, memory, and associated I/O, can be squeezed into a 3U VPX form factor.

The key to this development is the FPGA mezzanine card (FMC) and its newest iteration, FMC+. These industry-standard interface modules enable very-high-speed, direct I/O connections between the ADC/DAC devices lodged on the cards and the host FPGA, reducing end-to-end latency. There are many different FMC/FMC+ implementations, allowing customers the flexibility to meet their needs. What's more, the modules can easily be changed as higher-performance converters emerge and program needs grow. FMC+ accommodates up to 24 high-speed serial lanes and up to 80 parallel lanes, enabling massively wideband I/O. For EW applications like DRFMs, however, parallel interfaces are preferable to serial interfaces because of latency concerns.

An example of a multifunction, EW-optimized board is Abaco Systems' VP880, a 3U VPX FMC+ carrier card that features Xilinx's latest UltraScale FPGA and FPGA-hybrid Zynq UltraScale multiprocessor system-on-a-chip, along with 10 gigabytes of onboard memory. (Figure 1.)

Future challenges

EW technology has evolved over the years to include compute-intensive methods, as well as physical means such as chaff, decoys, and brute-force barrage jamming. The next step may be "cognitive EW," which uses machine learning algorithms to deploy adaptive and automated jamming techniques. The idea is that if one jamming technique is ineffective against a target radar, the EW system would instantly adjust the parameters to find a solution. This approach would require not only low-latency front-end processing but also powerful GPPs to run the more complex algorithms.

FPGAs, with their wide bandwidth, high throughput, and low latency, will continue to play a key role as EW technology evolves. Heterogeneous architectures, combining FPGAs, hybrid FPGA/GPPs, and even graphics processors, may also be necessary. They could allow the same data to be sifted through multiple processing chains simultaneously or for different purposes, serving the needs of more advanced, next-generation systems. Underlying it all is the flexibility of industry-standard COTS parts that can be combined in novel ways to meet emerging threats.

www.abaco.com

Taking the complexity out of PCI Express configuration to optimize HPEC system design

By Aaron Frank

An industry perspective from Curtiss-Wright Defense Solutions

Performance is all about eliminating bottlenecks to minimize latency and maximize throughput. Today's high-performance embedded computing (HPEC) systems integrate powerful processing subsystems, each of which might be a fully functional processing node needing to share data with other processing nodes. To maximize overall system performance requires the fastest, most efficient processor-to-processor data paths. With VPX, embedded systems moved away from the VMEbus shared parallel bus model.

Compared to today's serial fabric-based systems, VME performance suffers from low overall throughput. One cause is slow data bus transfer speeds. Another problem is the bus arbitration penalty that occurs when only one node can communicate at a time. For modern serial architecture-based systems like VPX, Ethernet can also be used to pass data from node to node. Switched Ethernet architectures enable nodes to communicate in parallel, all but eliminating the bottlenecks of a shared bus. However, processor speeds and capabilities today far outpace Ethernet speeds, making data paths and the CPU-intensive networking stack a key performance bottleneck yet again.

Other alternative fabrics, such as Serial RapidIO (SRIO) and InfiniBand, have their own limitations: Few silicon vendors support SRIO, which means that its adoption has been hindered by lack of software. Because no common software API [application programming interface] for SRIO has been widely adopted, system designers have typically needed to write their own custom software. Operating system support for SRIO has also been scarce, making SRIO device drivers also a custom development. For its part, InfiniBand also has limited appeal in deployable defense systems due to limited software support for real-time operating systems. It's also hindered by the high cost of silicon devices and limited support from its single-source vendor.

Today, almost every contemporary processor uses the PCI Express (PCIe) bus as a high-speed interconnect for onboard peripherals. In most processing systems, the PCIe interface also offers the fastest data path to and from the processor. The PCIe

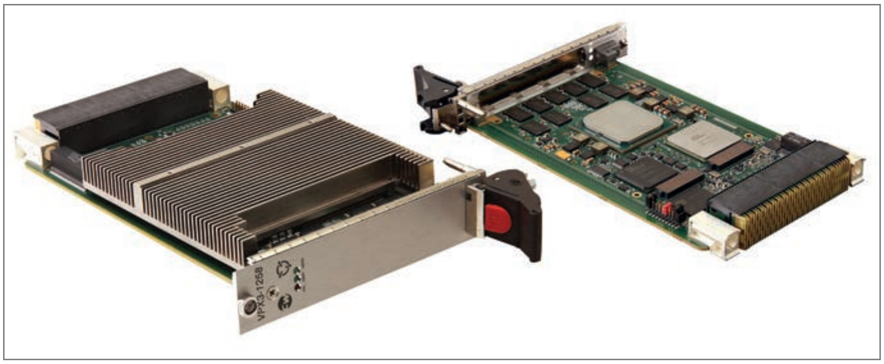


Figure 1 | Curtiss-Wright's VPX3-1258 and CHAMP-XD1 are examples of single-board computers that support PCIe.

interface supports several data rates: Gen1 interfaces run at 2.5 Gbps, with Gen2 interfaces doubling the data rate to 5.0 Gbps. Gen3 interfaces increase this speed to 8.0 Gbps, and by using a more efficient data-coding mechanism, the effective data-transfer rate becomes double that of Gen2. The development of the PCIe Gen4 standard is just about complete, and Gen4 devices will begin to ship from vendors later in 2017, again aiming at doubling performance.

Why use PCIe to bypass Ethernet or other fabric interface devices? Users report lower latency, increased throughput, and additional side benefits such as reduced power dissipation, increased MTBF [mean time between failures], and lower costs. Until recently, however, the benefits of using PCIe technology to support host-to-host communications required complex setup and the configuration of PCIe devices and switches. It also called for custom PCIe shared memory driver software, greatly diminishing its desirability.

Dolphin Interconnect Solutions, known by many for its StarFabric technology, has developed a solution with great promise for HPEC systems. Its eXpressWare software suite uses PCIe connections to create faster and more flexible message and processor-to-processor communications data-transfer mechanism. The software is optimized to take advantage of hardware features such as DMA [direct memory access], PCIe multicast, and multicore processing. The software hides the complexities of PCIe setup, which simplifies the setup and configuration of host-to-host architectures.

When supported with all the required PCIe switch configurations, the software can automatically detect and configure PCIe endpoints as transparent or nontransparent ports, set up message queues and data-transfer windows, and configure and manage data-transfer resources such as DMA engines. In addition, it comes with standard software API interfaces, which enables faster software application development with software paradigms already familiar to most software developers.

Dolphin's eXpressWare enables HPEC system designers to exploit the highest levels of data fabric performance for the defense industry's ruggedized equipment needs. To reap the benefits of using PCIe for node-to-node data transfers to embedded system designers, Curtiss-Wright has recently added support for eXpressWare to embedded Intel SBCs and DSP engines running both Linux and Wind River VxWorks operating systems, and have also extended that support to Power Architecture-based boards (Figure 1). Rugged embedded systems depend on high-performance fabrics to reduce latency in data-transfer times. PCIe offers today's best solution for realizing low latency, high throughput processor-to-processor performance. By providing common software APIs and masking the complex details of programming PCIe devices, eXpressWare delivers a breakthrough for HPEC system designers and brings high-speed, low-latency, peer-to-peer communications to embedded hardware.

Aaron Frank is the Senior Product Manager, Intel SBC, for Curtiss-Wright Defense Systems.

www.cwcdefense.com

DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Mariana Iriarte, Associate Editor

NEWS

UUV completes underwater mine-hunting trials

General Dynamics Mission Systems reports that it has successfully completed a comprehensive evaluation of Knifefish, an autonomous surface mine countermeasure (SMCM) unmanned undersea vehicle (UUV), in coordination with the U.S. Navy.

The Knifefish tests were held in the ocean near Boston using submerged Navy mine test targets. The UUV simulated mine-hunting missions as it located and classified mine test targets submerged at various depths and on the sea floor. General Dynamics says that Knifefish is also capable of locating and identifying mines that are buried in the sea floor.

According to the company, Knifefish will reduce risk to personnel by operating in the minefield as an off-board sensor while the host ship is able to remain outside the boundaries of a potentially hazardous minefield.

Figure 1 | The test events took place off the coast of Boston using submerged Navy mine test targets. Photo courtesy of General Dynamics Mission Systems.

Leidos selected to expand emerging open systems architecture standards in AFRL program

The Air Force Research Laboratory (AFRL) tasked Leidos to provide research and development (R&D) under an initial task order for the Mission Systems Open Architecture Science and Technology (MOAST) Program. The contract has a seven-year performance period and has a total shared ceiling value of approximately $48 million.

Under the MOAST program, Leidos will perform R&D to help evolve and expand emerging open systems architecture standards for existing and next-generation Air Force and Department of Defense (DoD) weapon systems, while also ensuring or enhancing cyber resilience.

Work for the multiple award, indefinite delivery/indefinite quantity (IDIQ) contract will be performed primarily at Wright-Patterson Air Force Base.

ONR awards Raytheon $11.8 million contract for work on sensor interconnectivity

The U.S. Office of Naval Research (ONR) has awarded Raytheon a contract worth $11.8 million to develop networking technologies that will enable enhanced sensor interconnectivity and improved integrated-fires capabilities for naval operations.

The network, called Communications and Interoperability for Integrated Fires (CIIF), will advance situational awareness for forcewide integrated air and missile defense. New and existing ships, planes, unmanned aerial vehicles (UAVs), and expeditionary forces will communicate and share critical information across data links; these links connect one platform to another through radio frequency to transmit and receive digital information.

CIIF will leverage existing and planned sensor networking systems deployed onboard both naval ships and aircraft, and also in U.S. Marine Corps expeditionary systems and land-based test sites.

Teledyne awarded $9.98 million to supply IR detectors for Jupiter mission

Teledyne Scientific & Imaging, a Teledyne Technologies subsidiary, has been awarded a $9.98 million contract from the French Space Agency – the Centre National d'Études Spatiales (CNES) – to provide infrared (IR) detectors and electronics for the European Space Agency (ESA) JUICE mission to Jupiter.

JUICE – the ESA's acronym for JUpiter Icy moon Explorer – is expected to launch in 2022 and reach Jupiter in 2030 to undertake a three-year study of Jupiter and three of its moons: Callisto, Ganymede, and Europa.

Teledyne is tasked with delivering infrared detectors and focal plane electronics to the Institut d'Astrophysique Spatiale (IAS) for use in the MAJIS spectrometer aboard the mission. Teledyne intends to deliver the detectors and electronics to the IAS within 24 months.

Figure 2 | JUICE is the ESA's acronym for JUpiter Icy moon Explorer. Artist's rendering of the JUICE mission courtesy of ESA/AEOS.

DARPA working on program to enable airborne UAS launch-and-recovery system

The Defense Advanced Research Projects Agency (DARPA) recently completed Phase 1 of its Gremlins program, which has as its goal fielding volleys of low-cost, reusable unmanned aerial systems (UASs) that would be launched and later retrieved in midair. Moving on to the next stage, DARPA has now awarded Phase 2 contracts to two teams, one led by Dynetics (Huntsville, Alabama) and the other led by General Atomics Aeronautical Systems (San Diego, California).

The Gremlins program envisions launching groups of UASs from multiple types of military aircraft, including bombers, transport, fighters, and unmanned fixed-wing platforms, while out of range of adversary defenses. When the "Gremlin" UASs complete their mission, a C-130 transport aircraft would retrieve them in the air and carry them home, where ground crews would prepare them for their next use, as soon as within 24 hours.

Because the Gremlin UASs would be reusable, with an expected lifetime of about 20 missions, the system could reduce payload and airframe costs while also lowering mission and maintenance costs over that of conventional manned platforms.

Figure 3 | Artist's concept of the Gremlins program. Image courtesy of DARPA.

Aptima and Milcord merger focuses on human-centered engineering for defense, intel

Aptima has announced its merger with Milcord, a government-technology company based in Waltham, Mass., specializing in knowledge management, human social-culture modeling, and cyberdefense.

Under the agreement, Aptima will acquire Milcord's portfolio of completed, active, and pending contracts and intellectual property developed under these contracts; the merged entity will continue under the Aptima corporate umbrella.

Since its founding in 1995, Aptima has handled more than 800 knowledge-management contracts throughout the Department of Defense (DoD). One of Milcord's notable programs is the Marine Civil Information Management System (MARCIMS), the U.S. Marine Corps knowledge-management system for global disaster and humanitarian missions.

Global defense and aerospace revenues likely to rise during 2017, say analysts

The global aerospace and defense (A&D) sector is likely to experience stronger growth in 2017, following multiple years of positive yet subdued growth, say analysts with multinational professional-services firm Deloitte. In its market report, "2017 Global Aerospace and Defense Industry Outlook," Deloitte forecasts that A&D sector revenues will likely grow by about 2 percent in 2017.

Defense subsector revenues, according to the report, are likely to grow at a much faster 3.2 percent in 2017, as defense spending in the U.S. has returned to a growth position, following multiyear declines in defense budgets.

On the defense side, Deloitte sees a resurgence of global security threats, expected increases in U.S. defense budgets, and higher defense spending from other major regional powers such as Japan and India as likely promoting global defense subsector revenue growth in the near future. The report calls out in particular an upside for U.S. defense expenditures, given the outcome of the recently concluded U.S. elections.

MS-177 sensor payload begins testing on RQ-4 Global Hawk

Engineers at Northrop Grumman Corp. have started testing the MS-177 sensor payload on an RQ-4 Global Hawk aircraft system. The flight tests are the first time the sensor has flown on a high-altitude long-range autonomous aircraft, officials say. Testing is expected to continue through the first half of 2017.

The MS-177 sensor is designed to provide capabilities such as finding targets by using broad-area search and various sensing technologies. Other capabilities include tracking and assessing targets through its multiple sensing modalities.

The Global Hawk system, in active operation with the U.S. Air Force since 2001, has amassed more than 200,000 flight hours, with missions flown in support of both military and humanitarian operations.

Figure 4 | Northrop Grumman's Global Hawk aircraft begins flight tests of its sensor payload. Photo courtesy of Northrop Grumman.

NASA reveals work on tiny folding robots for exploring extreme terrains

NASA and several partners are working on what the space agency calls an "origami-inspired" small robot that can fold itself to become as small as a smartphone but is rugged enough to handle harsh terrain on Mars and beyond.

The PUFFER robot – the acronym stands for "Pop-Up Flat Folding Explorer Robots" – will be designed for small size, light weight, and extreme flexibility, making it an option for exploring some of the harshest landscapes in the solar system. The project is still in development as an 18-month-long collaborative project involving NASA's Jet Propulsion Laboratory, University of California Berkeley, and optical and sensor technology company Distant Focus Corp. (Champaign, Illinois).

The next phase for the PUFFER project and partners is testing in the Mojave Desert during 2017, to simulate the harsh Martian atmosphere. To see videos of the PUFFER test in action, visit the NASA Game Changing Development page at gameon.nasa.gov.

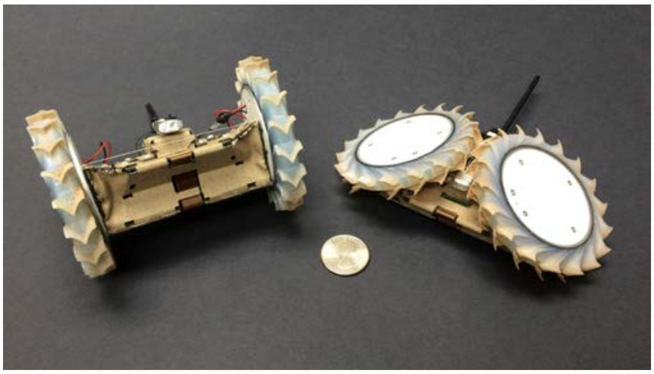


Figure 5 | The PUFFER's small size and low cost would allow a "parent" spacecraft to carry and deploy many on a single mission. Photo courtesy of NASA.

Georgia Tech pairs with firm to build military jetpack

JetPack Aviation (JPA) has entered into a development agreement with the Georgia Institute of Technology (Georgia Tech) to design and build a soldier vertical-mobility system (SVMS) for military applications.

Under the agreement, JPA has begun initial work with the U.S. Navy under a Cooperative Research and Development Agreement (CRADA) to provide its proprietary jetpack technology, while Georgia Tech will contribute advanced electronic subsystems for the new SVMS.

Working under a grant from the Georgia Tech Research Institute, the early development stage of the SVMS project has focused on three specific subsystems: an autonomous control system, a pilot exoskeleton, and a heads-up display (HUD) helmet for the pilot.

DoD awards $47 million in research grants

The Department of Defense (DoD) has announced awards totaling $47 million to 160 university researchers at 84 institutions, through its Defense University Research Instrumentation Program (DURIP). DURIP supports the purchase of state-of-the-art equipment for universities as they conduct cutting-edge defense research and associated graduate-student research training.

Pertinent research at U.S. colleges and universities forms the basis of advances in materials, structures, and manufacturing science; quantum and nanosciences; computing and networks; electronics, electromagnetics, and electro-optics; acoustics; neuroscience; fluid dynamics; robotics and artificial intelligence; and ocean, environmental, and life sciences.

The DURIP awards are administered through a merit competition conducted by the Army Research Office, Office of Naval Research, and Air Force Office of Scientific Research; solicited proposals target university investigators conducting science and engineering research of importance. Individual awards range from $53,000 to $1.4 million, with an average of approximately $300,000 per award, according to the DoD.

Lockheed Martin tests updated JASSM

Lockheed Martin announced that its updated Joint Air-to-Surface Standoff Missile (JASSM) recently completed two successful verification flight tests at White Sands Missile Range in New Mexico.

The most recent tests were intended to demonstrate JASSM's updated Global Positioning System (GPS) antijam hardware and software, verifying operation in both GPS-degraded and nonjammed environments. During the White Sands test, B-2 and B-52 bomber aircraft launched the JASSM missiles at altitudes greater than 24,000 feet. Lockheed reports that the missiles navigated to and destroyed their intended targets, completing all mission objectives.

JASSM and its extended-range sibling (JASSM-ER) are armed with a penetrating blast-fragmentation warhead that is made to operate in all weather conditions. These cruise missiles also incorporate an infrared seeker to dial into specific points on targets.

Figure 6 | JASSM is integrated on the U.S. Air Force's B-1B, B-2, B-52, F-16, and F-15E aircraft. Photo courtesy of Lockheed Martin/U.S. Air Force.

INDUSTRY STANDARDS

Sensor Open Systems Architecture (SOSA): an overview

By John McHale, Editorial Director

Ilya Lipkin

Budget cuts and sequestration, while handcuffing the defense industry and the warfighter, have also forced the government to embrace a movement toward more commonality across multiple platforms through open standards and establishing a culture of reuse. One such initiative, the Sensor Open Systems Architecture (SOSA), creates modular open systems architecture specifications to enable reuse of key sensor components across multiple platforms and services. In this Q&A with Dr. Ilya Lipkin, Lead Manager for SOSA at the U.S. Air Force Life Cycle Management Center, he explains SOSA, its similarities to other initiatives like the Future Airborne Capability Environment (FACE), how standards organizations like VITA are involved, and why today's procurement environment is so open to initiatives such as SOSA.

MIL-EMBEDDED*: Please provide a brief description of your responsibility within the Air Force Life Cycle Management Center (AFLCMC) and its overall role within the Air Force?*

LIPKIN: My responsibilities within the Air Force are to support existing programs and our acquisition activities at AFLCMC for Intelligence, Surveillance, Reconnaissance, & Special Operations Forces Directorate. Within the Air Force, AFLCMC is one of six centers under Air Force Materiel Command; the Air Force Life Cycle Management Center is the single center responsible for total life cycle management of Air Force weapon systems. The AFLCMC Mission: "Acquire and Support War-Winning Capabilities" Its Motto: "AFLCMC ... Providing the Warfighter's Edge" (source www.wpafb.af.mil/aflcmc).

MIL-EMBEDDED*: What is the Sensor Open Systems Architecture (SOSA) and why was it created?*

LIPKIN: The Sensor Open System Architecture (SOSA) effort was created to develop a series of modular open systems architecture specifications for a variety of multi-intelligence C4ISR [command, control, communications, computers, intelligence, surveillance and reconnaissance] platforms that cross services and platform environment. Specifically, SOSA is business/acquisition practices and a technical environment for sensors and C4ISR payloads that foster innovation, industry engagement, and competition, and allow for rapid fielding of cost-effective capabilities and platform mission reconfiguration while minimizing logistical requirements for the following set of initial modalities: radar/synthetic aperture radar (SAR), SIGINT [signals intelligence], electronic warfare (EW), communications, and electro-optics/infrared (EO/IR). The SOSA initiative is being incubated as part of the FACE consortium of The Open Group, and is going through activities to create attractive business and technical draft snapshot products to stand up as part of an ecosystem of related and relevant standards that work together.

MIL-EMBEDDED*: How is SOSA similar to the Navy's FACE effort and the Army's Open Mission Systems (OMS)?*

LIPKIN: SOSA is a complementary effort that functions seamlessly with FACE and OMS. SOSA is inherently agnostic to FACE and OMS. The SOSA Software Working Group is developing an architecture that could, quite possibly, heavily leverage both FACE and OMS. Furthermore, there are other open architecture initiatives that are being considered for SOSA to leverage, for example, REDHAWK, MBE-RF, SAE SPIE, VITA, and many other initiatives across software, hardware, and electrical interfaces.

MIL-EMBEDDED*: What is the timetable for seeing SOSA-compliant architectures/interfaces in deployed systems? Are there any programs already adopting SOSA?*

LIPKIN: Currently SOSA is about one year old, and it will take some time to develop relevant standards. However, the snapshot of several SOSA-compliant architectures/interfaces should be released over the next couple of month for areas that we feel are mature to be inserted for consideration into existing programs of record as either part of the upgrade, or new starts, with incremental development strategy. Hence, a lot of SOSA activities are based on existing industry-supported standards. I am confident that we can release SOSA specifications as soon as consensus is reached on the right technologies to push forward.

The challenge is that there are many open architectures and choosing the right one is the key for a 30- to 40-year life cycle implementation into our systems. Currently there is one program that has adopted SOSA, AFRL's AgilePod T Program – a proof of concept Multi-Int ISR, reconfigurable, open architecture developmental platform. We are using AgilePod to help validate certain elements of the SOSA architecture and standards for eventual integration into operationally fielded platforms. Furthermore, there are small-business innovation research opportunities for SOSA development through the AFRL portal, with more being planned for the future. (Figure 1).

MIL-EMBEDDED*: How does SOSA leverage the work being done with the Navy's Hardware Open Systems Technology (HOST)?*

LIPKIN: The SOSA Hardware Working Group is leveraging NAVAIR's HOST effort via adoption of HOST's existing module, backplane, and slot profiles. This also leverages an ongoing hardware-convergence effort between the Air Force, Army, and Navy. Each slot profile and module profile will get used in the SOSA architecture.

MIL-EMBEDDED*: Which current and in-development VITA standards will be leveraged within SOSA?*

LIPKIN: These existing standards are leveraged: VITA 65, VITA 46, VITA 48, VITA 48.2, VITA 62, VITA 49, and VITA 49.2.

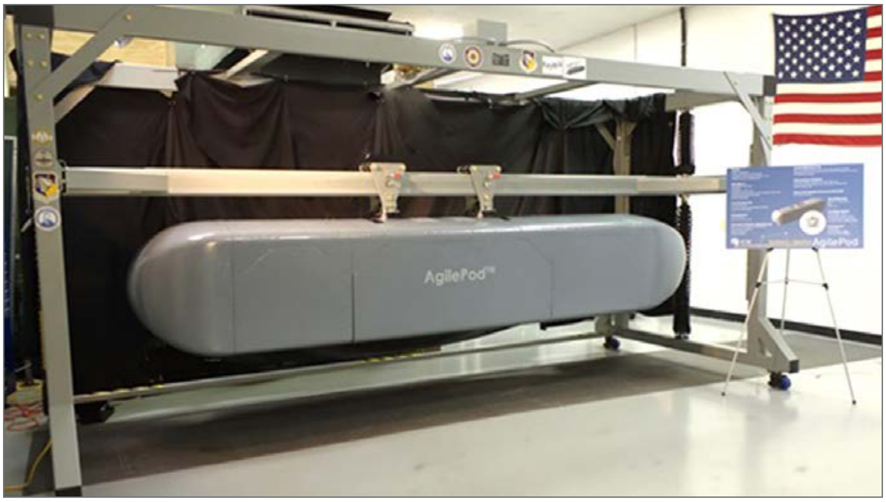


Figure 1 | Air Force Research Laboratory's AgilePod is a multi-intelligence, open architecture, reconfigurable prototype designed for the intelligence, surveillance, and reconnaissance (ISR) and Air Force Special Operations communities. The reconfigurable pod enables operators to customize sensor packages based on specific mission needs, enhancing the intelligence process. The AFRL's AgilePod T Program is the first to have adopted SOSA; the AFRL is using AgilePod to help validate certain elements of the SOSA architecture and standards for eventual integration into operationally fielded platforms. The pod capability will be tested on a medium-altitude MQ-9 surrogate aircraft in May 2017. (Air Force courtesy photo/released.)

MIL-EMBEDDED***: Are there other standards bodies aside from VITA you are working with on SOSA?***

LIPKIN: I believe there is a relationship between The Open Group and SAE as well, therefore some of the standards chosen to move forward are part of SAE.

MIL-EMBEDDED***: Why is the climate within the Department of Defense (DoD) community today more conducive to efforts such as SOSA and FACE than in the past? More collaboration? Or is it a result of budgetary pressures forcing more commonality?***

DISPARATE GROUPS AND ENTITIES HAVE SEEN, INDEPENDENTLY, THE BENEFIT OF MOVING TO A MODULAR OPEN ARCHITECTURE ENVIRONMENT FOR A WIDE VARIETY OF APPLICATIONS.

LIPKIN: The DoD and government community realizes that current and future systems are growing in complexity. Disparate groups and entities have seen, independently, the benefit of moving to a modular open architecture environment for a wide variety of applications. There is a convergence of applications that are data- and information-driven. This, in turn, drives commonality across hardware and software modules.

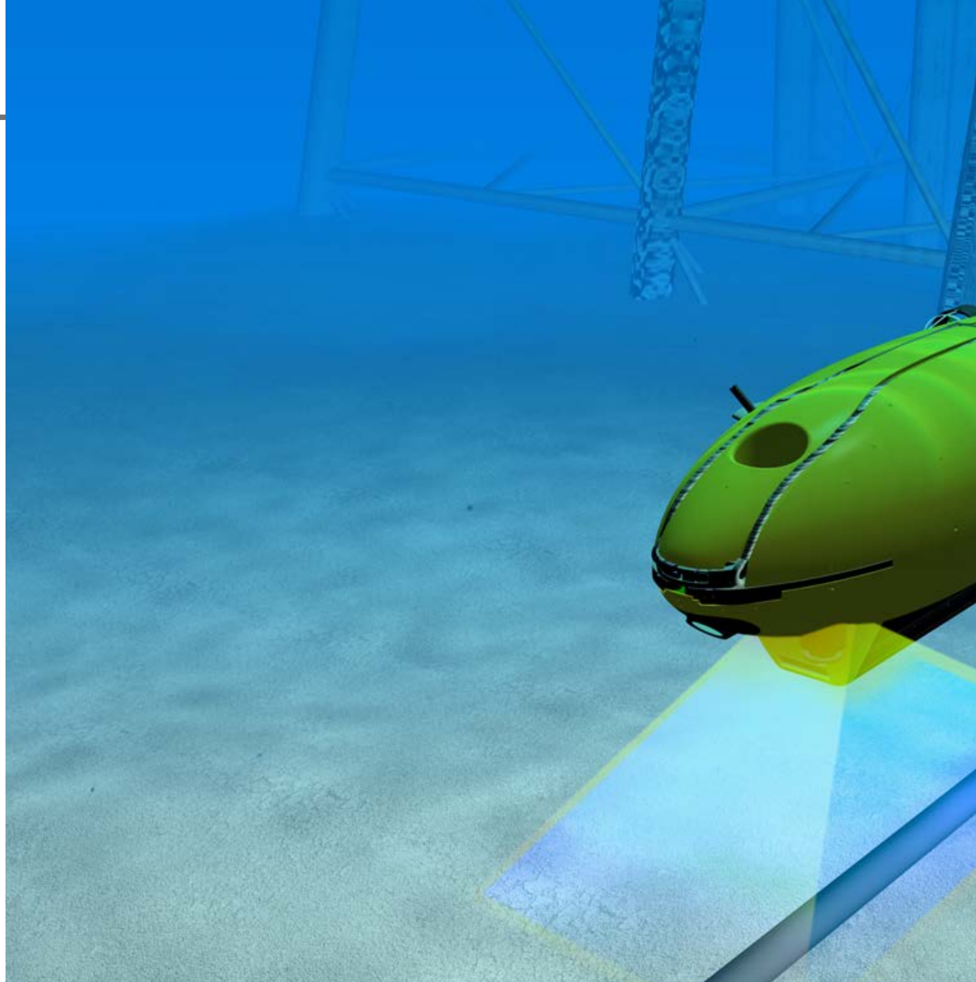
MIL-EMBEDDED***: Where online can readers learn more about SOSA?***

LIPKIN: Currently, to gain detailed information on SOSA requires membership in the FACE Consortium; however, after incubation activities are completed, the snapshots and technical standard will be available from The Open Group in the exact same way as FACE: www.opengroup.us/sosa. **MES**

__Dr. Ilya Lipkin__ is a project software engineer for the U.S. Air Force Life Cycle Management Center (AFLCMC). Previously he was assigned to Hill Air Force Base 309th SMXG where he developed embedded drive-by-wire software systems for Expeditionary Fighting Vehicle (EFV). His next assignment was at AFLCMC Wright-Patterson AFB where he led MQ-1/MQ-9 and Global Hawk Training Systems. He is a member of the AFLCMC software working group AFSIP, Future Airborne Capability Environment (FACE), and Sensor Open Systems Architecture (SOSA) working groups. His current research interests are in automated machine-learning and pattern-recognition algorithms, software architecture, and multi-INT sensor decomposition. Dr. Lipkin has numerous publications in Journal of Defense Software Engineering Crosstalk, IITSEC, and Decision Sciences Journal as well as numerous conferences. He has an MSE in computer engineering from the University of Michigan, an MBA in Operations Management, and a PhD in Software Project Productivity from University of Toledo. He is currently assigned to AFLCMC/WING and SOSA, where he leads development efforts in partnership with AFRL for SAR and HSI compression, as well as heading SOSA Consortia for the U.S. Air Force.

Unmanned undersea vehicles are "embracing nature" and evolving quickly

By Sally Cole, Senior Editor



Lockheed Martin's Marlin unmanned undersea vehicle can carry out a variety of military and commercial missions. Image courtesy of Lockheed Martin.

Unmanned undersea vehicles (UUVs) are pushing boundaries and evolving in innovative ways – often drawing design inspiration from nature – to carry out a variety of military missions.

By drawing design inspiration from nature, unmanned undersea vehicles (UUVs) are evolving to become downright innovative and stealthy and, in many cases, capable of carrying payloads that can be customized for a wide variety of military missions.

One of the most well-known UUVs is Lockheed Martin's Marlin, which is capable of fully independent operation. The U.S. Navy can use Marlin "for a variety of undersea applications such as below water intelligence, surveillance, reconnaissance, and small payload deliveries," says Tim Fuhr, director of autonomous maritime systems for Lockheed Martin. "Marlin can go where submarines and manned vessels can't or don't want to go, and use its sensors, communication, and data reduction capabilities."

Sea mines are one of the most formidable challenges the Navy faces, and finding and mapping them "is good usage of UUVs," Fuhr says. "UUVs like Marlin can be outfitted to be a single-sortie detect-to-engage chain, coupled with the right sensors, target recognition software, and an expendable mine neutralizer."

Another well-known UUV is "Knifefish," which was created by Bluefin Robotics Corp. and has since become part of General Dynamics Mission Systems. Its standard model uses a wide variety of sensors to conduct its operations, including inertial navigation systems, Doppler velocity logger, compasses, and sound-velocity sensors. Knifefish's payload is a low-frequency broadband synthetic aperture sonar to detect buried mines.

"Knifefish provides search, detection, classification, and identification of buried, bottom, and volume mines in high-clutter environments in a single pass – with minimal intervention by human operators and reduced overall mine countermeasures mission timeline," says Matt Graziano, a director of the Maritime and Strategic Systems line of business within General Dynamics Mission Systems. "The proliferation of relatively low-cost and easily deployed underwater mines poses a unique threat to naval operations and maritime security." (Figure 1.)

UUV payloads

As far as payloads being carried by UUVs, the ability to customize for specific missions is highly desirable. "We have multiple Marlin vehicles, and each is outfitted slightly differently with COTS [commercial off-the-shelf] parts, custom sensors, and communications electronics," Fuhr notes. "It's straightforward to customize the vehicles for a particular application as long as the electronics are compatible with

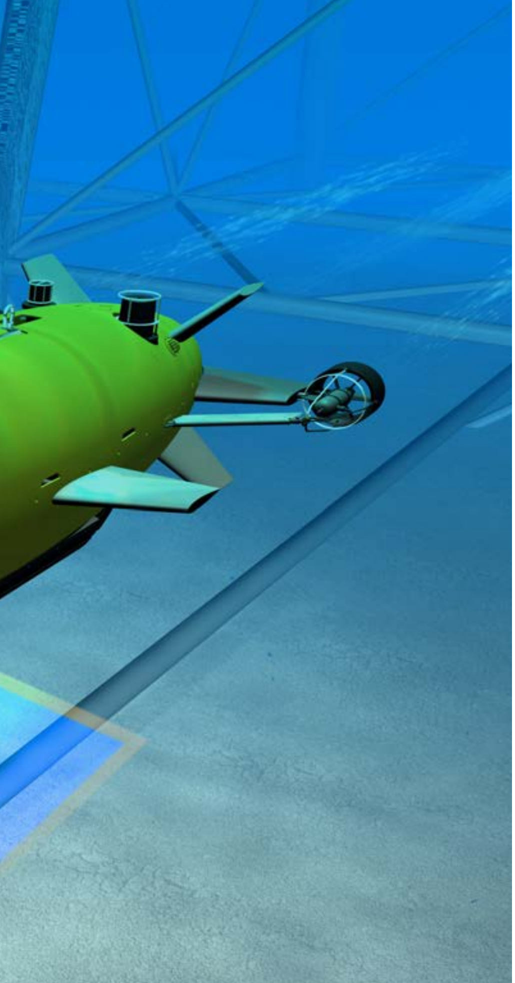


Figure 1 | The Knifefish UUV was developed by Bluefin Robotics Corp., which is now part of General Dynamics Mission Systems. Image courtesy of General Dynamics Mission Systems.

Marlin's size, weight, and power (SWaP) requirements."

"Autonomy, data-processing capabilities, energy systems, and underwater communication systems are the main areas of development and challenge," in UUV development today, according to Fuhr. "Energy-storage systems define the size of UUVs because the vehicle must carry its own energy source, which has to last for the duration of an intended mission. A UUV like Marlin wants to maximize mission range, minimize detectability, and have the capacity to be a data and communications node – in both single-asset and multiple-asset mission scenarios."

Where is UUV technology heading next? Lockheed Martin is focusing on "coordinated development of extra-large UUVs for large payload capabilities; large-diameter systems for submarine-related operations; small UUVs for mine countermeasures and missions where expendability is desired; and cooperative behaviors between UUVs, unmanned surface vehicles (USVs), and unmanned aerial vehicles (UAVs)," Fuhr

says. "Another key element is interoperability with other assets, and the ability to enable and participate in multidomain operations."

Emerging innovations

Other defense prime contractors, government laboratories, and university teams are exploring innovations in the UUV realm. There are too many to note them all, but here are a few exceptional ones.

› Release the CRACUNS!

Seemingly something straight out of science fiction, researchers at Johns Hopkins University's Applied Physics Laboratory recently developed the Corrosion Resistant Aerial Covert Unmanned Nautical System, dubbed the CRACUNS, which is an unmanned aerial vehicle (UAV) that can stay on station hidden below water, and then launch into the air to perform a variety of missions. (Figure 2.)

The ability to "Release the CRACUNS" is ushering in new capabilities not previously possible with UAV or UUV platforms. Its ability to operate within the harsh littoral environment, as well as its payload flexibility, means that CRACUNS can be used for a wide array of missions. Its low cost is a bonus that makes it expendable, allowing for use of large numbers of vehicles for high-risk scenarios.

The most innovative feature of CRACUNS? The researchers say that it can remain at and launch from a significant depth or from a UUV without needing structural metal parts or machined surfaces. To do this, the designers fabricated a lightweight, submersible, composite airframe capable of withstanding water pressure while submerged. Sensitive components are protected from a corrosive saltwater environment by being sealed within a dry pressure vessel, while motors receive protective coatings.

Figure 2 | CRACUNS can be launched from a fixed position underwater or from an unmanned undersea vehicle. Image courtesy of Johns Hopkins Applied Physics Laboratory.

› Undersea navigation

Another key advance currently underway is focused on undersea navigation. BAE Systems is working to develop an undersea navigation system for the U.S. Defense Advanced Research Projects

Can owl stealth be applied to underwater vehicles?

Owl wings possess stealth features not found on other birds. People have been studying them for more than 80 years to try to identify what exactly makes owl flight virtually silent.

A group of researchers from Lehigh University, Virginia Tech, Florida Atlantic University, and the University of Cambridge (U.K.) are now exploring the acoustics of owl flight to determine whether so-called owl stealth can reach beyond improving the aerodynamic design of wind turbines, rotors, aircraft, and automobiles and apply also to applications for underwater vehicles. (Also see University Update, p. 44.)

Three key features of owl wings contribute to their stealth, according to Justin W. Jaworski, assistant professor of mechanical engineering and mechanics at Lehigh University's P.C. Rossin College of Engineering and Applied Science. [Sidebar figure 1.]

This includes "a leading-edge comb composed of little bristles that point into the flow at the front of the wing; a trailing-edge fringe that creates a poorly defined edge that's porous and compliant; and a downy layer on the upper wing's surface," he explains. "If you run your hand along the top of an owl wing, you'll find that it has a velvety texture – this feature is the least well understood part of the owl wing."

The hope is that by gaining an understanding of how owl wings operate in air, the physical mechanism can then be adapted to water.

Jaworski is developing math models to decipher the aerophysics involved, while also collaborating with William Devenport, Nathan Alexander, and Ian Clark at Virginia Tech; Stewart Glegg at Florida Atlantic University; and Nigel Peake at the University of Cambridge on the hydroacoustics side to work together to refine the math models and experiments.

After determining that the structure of the owl wing's downy, velvety surface might be modifying the flow upstream of the trailing edge in a way that suppresses noise, the group came up with an invention they call "finlets," which are essentially 3-D-printed wing attachments that mimic the downy canopy on the surface of owl feathers. [Sidebar figure 2.]

One way owl wings reduce noise is "by reducing the coherence of the spanwise coherence of the turbulence at the trialing edge," Jaworski says. "If you break that coherence up, the turbulence noise scattered by the edge is weakened. Small finlets can be retrofitted or 'pasted' onto the top to do this, so to speak."

What did the team discover via wind-tunnel testing? By installing finlets on a wind turbine blade, the trailing-edge noise over a broad range of frequencies from 1 to 4 kHz – where human hearing is most sensitive – can be reduced by an amazing 10 dB. Humans hear on a logarithmic scale, so a 10-dB reduction means that finlets cut the perceived sound in half.

"The aerodynamic tests, also carried out by my collaborators at Virginia Tech, measured the lift and drag characteristics with and without finlets. It turned out that finlets help maintain lift and keep the wind turbine blade from stalling at high angles of attack," Jaworski says. "A modest increase in drag occurs that's commensurate, with the increased surface area due to the addition of finlets … but there isn't a dramatic drag increase. The overall effect of installing finlets is a remarkable noise reduction at surprisingly minimal aerodynamic impact."

As far as technical challenges facing the finlets, "ensuring they'll work underwater is an open technical question worth exploring," Jaworski notes. "Can they stay attached? Biofouling is an issue underwater, so is it even feasible? It's a technical question as much as a design question to determine whether it can actually work."

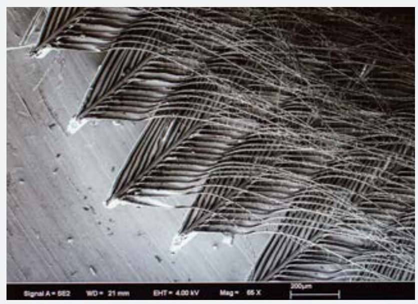
Another question is: "Can it work in an underwater environment as it is now, or would we need to be more clever to figure out how to make it work underwater?" he continues. "If the physics works, but it doesn't work long-term in the real world because you need to send someone down to clean it off every week … other approaches may be needed to help make it happen."

What does the future hold in terms of military applications for owl stealth technology? "It'd be nice to be able to use this passive means of modifying turbulence – in conjunction with other design strategies to reduce the noise – for aerial and underwater vehicles," Jaworski says.

Sidebar Figure 1 | This image shows a Eurasian eagle owl feather, where the three unique owl wing features (leading-edge comb, trailing-edge fringe, and downy upper-wing surface) can be observed on an individual feather. Image courtesy of Lehigh University.

Underwater swimming robots are another area of interest for the team, because robots like these would possess a noise signature as well. "Can we disguise these noise signatures so they sound like a tuna? A potential signal-processing aspect is being able to understand and predict the noise signal from swimming robots or to have them mimic actual underwater signatures of fish or schools of fish … and the ability to parse it from real fish," Jaworski adds. "But that's maybe 15 to 20 years down the road."

The group's work, not surprisingly, is partly funded by the Navy.



Sidebar Figure 2 | Scanning-electron microscope image of the downy surface on top of a barn owl's wing, which inspired the finlet design. Image courtesy of Lehigh University.

Agency (DARPA) to provide precise global positioning throughout the ocean basins. (Figure 3.)

The Positioning System for Deep Ocean Navigation (POSYDON) program's goal is to enable underwater vehicles to accurately navigate while remaining below the ocean's surface. Intriguingly, POSYDON will tap some hardcore physics to create a positioning, navigation, and timing system designed specifically to permit vehicles to remain underwater by using multiple, integrated, long-range acoustic sources at fixed locations around the oceans.

BAE Systems has more than 40 years of experience developing underwater active and passive acoustic systems: "We'll use this same technology to revolutionize undersea navigation for POSYDON by selecting and demonstrating acoustic underwater GPS sources and corresponding small-form-factor receivers," says Joshua Niedzwiecki, director of Sensor Processing and Exploitation for BAE Systems.

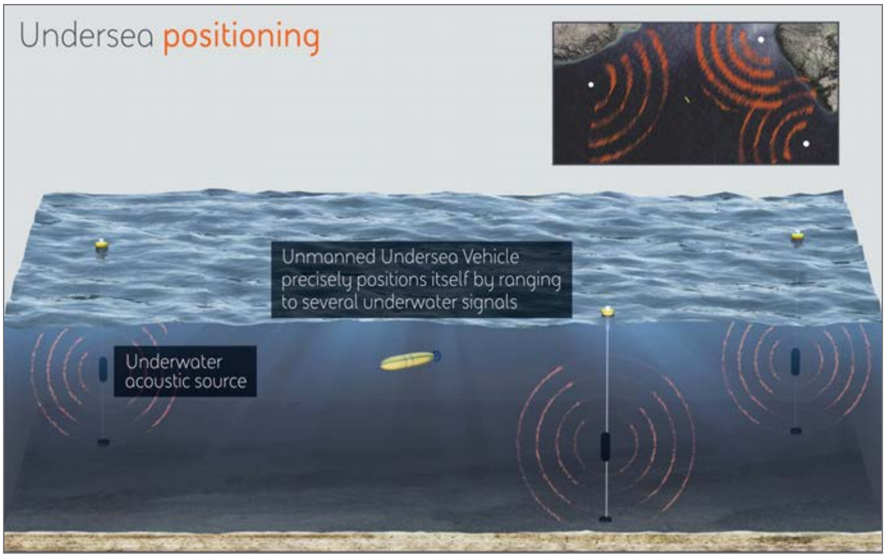


Figure 3 | BAE Systems is developing an undersea navigation system, called POSYDON, for DARPA, with the goal of allowing undersea vehicles to navigate below the ocean's surface. Image courtesy of BAE Systems.

The vehicle instrumentation that will be needed to capture and process acoustic signals will also be developed as part of the program. BAE Systems plans to use its capabilities in the areas of signal processing, acoustic communications, interference cancellation, and antijam/antispoof technologies. The company is collaborating with researchers from the University of Washington, Massachusetts Institute of Technology (MIT), and the University of Texas at Austin for the POSYDON program. **MES**

UNMANNED UNDERSEA VEHICLES & UNMANNED SURFACE VEHICLES

Designers of components for unmanned undersea vehicles (UUVs) are discovering that they don't have to reinvent the wheel – in general, standard military commercial off-the-shelf (COTS) embedded solutions can be specified in many cases for the undersea applications. Photo rendering courtesy Curtiss-Wright.

The commonality of COTS solutions for UUVs and UAVs

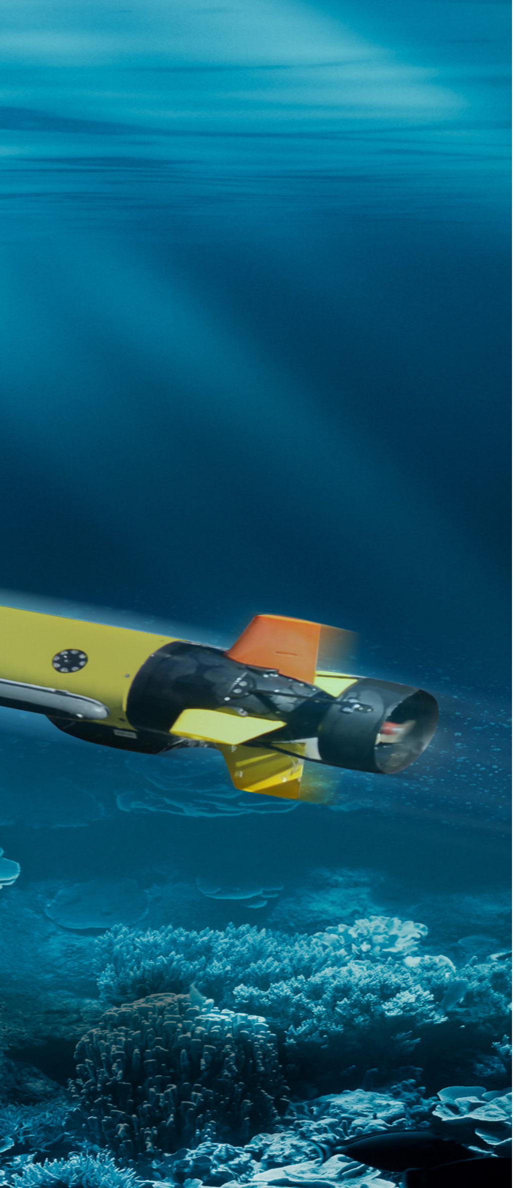
By Mike Southworth

Some time ago, when designers started thinking about unmanned undersea vehicle (UUV) applications, concerns were raised that the undersea environment might be so different or exotic that standard solutions would need to be significantly modified. To the surprise of many, however, it was found that there is significant commonality between unmanned aerial vehicle (UAV) and UUV environments. There are, to be sure, unique aspects to each type of platform, but in general, standard rugged military commercial off-the-shelf (COTS) embedded solutions are applicable to both.

The U.S. Navy sees great potential in the use of unmanned undersea vehicles (UUVs), which already see active duty today in such missions as searching for and removing mines and collecting oceanographic data. The range and scope of missions with which these platforms are tasked is sure to expand rapidly if the proliferation of uses for unmanned air and ground vehicles is any predictor.

According to a 2016 forecast from MarketsandMarkets, the overall UUV market – including commercial, defense, and homeland-security applications – is on track to nearly double, from $2.29 billion in 2015 to $4 billion by 2020. It's expected that these vehicles, whether small enough to be launched from a submarine's torpedo tubes or 51 feet long like Boeing's Echo Voyager, will take on more and more autonomy and will be sent on increasingly complex missions, such as intelligence, surveillance, and reconnaissance (ISR) and situational awareness. These types of compute-intensive applications will drive big increases in the amount of processing and networking capabilities that need to be deployed on UUVs. The good news is that many of the COTS solutions already developed, deployed, and field-proven on unmanned aerial vehicles (UAVs) are also suitable for use on UUVs. The challenge for UUVs, just as it is for their airborne and ground siblings, often comes down to size, weight, and power – especially power.

The trick for UUV system designers is how best to optimize the mission payload while taking into consideration the limits of the underwater vehicle's power source, which



THE GOOD NEWS IS THAT MANY OF THE COTS SOLUTIONS ALREADY DEVELOPED, DEPLOYED, AND FIELD-PROVEN ON UNMANNED AERIAL VEHICLES (UAVs) ARE ALSO SUITABLE FOR USE ON UUVs. THE CHALLENGE FOR UUVs, JUST AS IT IS FOR THEIR AIRBORNE AND GROUND SIBLINGS, OFTEN COMES DOWN TO SIZE, WEIGHT, AND POWER – ESPECIALLY POWER.

ultimately determines maximum endurance, distance, and speed. By definition, UUVs must travel through the thick medium of water, which means that it takes eight times the amount of energy to enable it to go twice as fast. That's why there's a technology race on to develop the best way to power UUVs. Power candidates today range from environmentally propelled wave gliders to electrical batteries, such as lithium-ion designs, to fuel engines and cells. Very recently, for example, Aerojet Rocketdyne received a contract from the U.S. Navy to develop technology that enables a UUV's battery to be wirelessly and remotely recharged while undersea.

COTS vendors have a big role to play in helping to expand the capabilities of UUVs by applying their expertise in miniaturizing electronics and ruggedizing for harsh environments. The SWaP constraints typical of UAVs are similar to those found in underwater vehicles. What's more, the same system architectures, technologies, module, and line-replaceable unit (LRU) approaches can be used to speed development and bring down cost. There are some differences, though, when deploying COTS systems undersea versus in the air. Some of those differences actually make life easier for the UUV designer and add requirements distinct from those confronted by airborne system integrators.

Cool it

It's safe to assume that for most COTS system designers the underwater environment is an unfamiliar one. It may come as a happy surprise, then, to find out that the one of the biggest differences (and advantages) that UUVs have over air and ground vehicles is that they operate in what has been called the biggest heatsink in the world. As a result, providing efficient thermal management is much less troublesome underwater. In fact, for some designs, water can actually be allowed to flow through the interior of the UUV to directly cool isolated payload chambers.

Cooling is a challenge for UAVs for the simple reason that there are fewer molecules in the air at higher altitudes. In the case where UAV system requirements provide no airflow for cooling electronics, thermal management is more difficult. The upside for UUV system designers is that a COTS system built to operate at high altitude is also one that can be trusted to perform well underwater. In fact, cooling demands are much more rigorous for UAVs flown where there is no air than they are for systems deployed in a sealed chamber, as is the case with many UUV subsystems.

UUV system designers also don't have to worry about altitude. For airborne applications, altitude can be of concern because of its potential effect on components, such as electrolytic capacitors, which are susceptible to failure at higher altitudes. UAV system designers must make sure that they are using components that are altitude-rated for the intended usage. For example, helicopters are generally satisfied with a device that can operate as high as 15,000 feet, while a surveillance aircraft may need devices that can function at altitudes from 30,000 to 60,000 feet. Airborne COTS systems typically must pass MIL-STD-810 altitude testing in an altitude simulation chamber to validate operation at the altitude required by the intended application.

Different for UUVs: Shock testing

While altitude is not a requirement for UUVs, they may have very different shock and vibration requirements than UAVs. For example, UUV testing might require simulating the effects of a torpedo hit. Certifying for this type of threat means that UUV subsystems may need to prove reliability for the relevant frequencies covered by MIL-S-901D, a U.S. Navy standard for shock testing. In this case, the COTS solution intended for deployment onboard a UUV might need to survive a floating barge test, where it is exposed to an explosive shock. Or, alternatively, shock testing might involve a 901D hammer test, during which the electronics are hard-mounted against a metal plate and then struck with a large hammer-like pendulum device that creates massive amounts of G-forces.

SoCs across the board

Overall, there is a great amount of commonality in the requirements of COTS solutions for UUVs, UAVs, and even unmanned ground vehicles (UGVs). For example, all three platforms can use system-on-chip (SoC) technologies: Because SWaP is a key issue, the use of Intel and ARM-core SoC-based mobile class processors, which consolidate CPU, I/O, and memory controllers all within a single IC package – such as an Intel Atom 3800 series processor – is beneficial. Having the option to select a single chip that combines a processor, its companion chipset, and graphics processor (like with the Intel Atom), or to combine a higher performance CPU and integrated GPU (like with the Intel Core i7 products) helps to reduce space and weight for the physical boards and therefore the overall physical size of the system. Moreover, each of these architectures uses advanced power management technologies, making them much more efficient from a MIPS [millions of instructions per second] or FLOPS [floating-point operations per second] per watt perspective. For that reason, they are being used increasingly in applications, such as UUVs, where power sensitivity is present.

Figure 1 | The DuraNET 20-11 switch supports IEEE-1588 PTP, which is used in both UUV and UAV applications.

A good solution for UUV components are LRUs that cool through passive natural convection; in these, heat is radiated through the thermal mass of the chassis outward without any moving parts, liquid, or air flow. Because the chassis doesn't need to be bolted down for heat to be conducted downward to a cold plate, these types of subsystems are much easier to thermally manage and integrate and can be located in a much wider variety of places within a platform. An example of rugged LRUs that cool with natural convection are Curtiss-Wright's Parvus DuraCOR mission computers and DuraNET network switches (Figure 1).

Whether the platform is a UUV or UAV, the mission will typically require communications, computing, and sensors. The target environment, whether air, ground, or sea, will determine which types of sensors need to be supported. For example, a UAV would need FLIR [a forward-looking infrared camera], while a UUV would call for sonar. Although the payloads between the various types of vehicles will be different, the basic COTS electronics won't vary that much.

Another area of commonality between UUVs and UAVs appears to be the use of Ethernet as the network backbone of choice. The underlying infrastructure for both platforms will use the same traditional Ethernet interface connectivity and can be built using the same COTS building blocks. Additionally, IEEE-1588 Precision Timing Protocol (PTP) synchronization over the network is also increasingly a common trait between the undersea and aerial vehicles. **MES**

Mike Southworth *serves as product marketing manager for Curtiss-Wright Defense Solutions, where he is responsible for the small-form-factor rugged mission computers and Ethernet networking subsystem product line targeting size, weight, and power (SWaP)-constrained military and aerospace applications. Southworth has more than 15 years of experience in technical product management and marketing communications leadership roles. He holds an MBA from the University of Utah and a Bachelor of Arts in Public Relations from Brigham Young University.*

Curtiss-Wright Defense Solutions
www.cwcdefense.com

RF AND MICROWAVE TECHNOLOGY FOR UNMANNED SYSTEMS

An RQ-4 Global Hawk unmanned aerial system (UAS) soars through the sky to record intelligence, surveillance, and reconnaissance data. (Air Force courtesy photo.)

RF and microwave technology enabling multimission unmanned systems

By Mariana Iriarte, Associate Editor

The different roles that unmanned aerial systems (UASs) play – whether used for intelligence, surveillance, and reconnaissance (ISR), search-and-rescue missions, or photography – are prompting engineers to design more RF and microwave content into these systems to meet all the Department of Defense (DoD) as well as civilian requirements.

Increased intelligence, surveillance, and reconnaissance (ISR) demands don't come without engineering challenge. Today's ISR payload designers face challenges that range from boosting the digital domain to handling the electromagnetic spectrum. Radio-frequency (RF) and microwave technology play a large part in enabling and meeting those diverse requirements.

"We're seeing a lot of increased radio-frequency microwave (RFMW) content across the entire [UAS] market space, which includes everything from the upper-end copters though military systems, including those with global range and global endurance," says Sean D'Arcy, strategic marketing, Aerospace and Defense, at Analog Devices in Chelmsford, Massachusetts. "This ranges from a high-end quadcopter that may be used for law enforcement all the way up to something like a Global Hawk. Both military and civilian applications are experiencing growing needs in this area."

Sanjay Parthasarathy, senior vice president of strategy at Cobham Advanced Electronic Solutions in Washington, is also seeing an increase in UAS RF content. The increase "is trending higher primarily because of three things: communications, surveillance, and effects. There's more need for autonomy, more need for sensors – the RF and millimeter wave sensors – together with more frequency agility. Of course, longer persistence and survivability is critical to today's [UAS] applications," he says.

Military program managers also want more dynamic range from their RF and microwave systems. "Receivers need to acquire a wide range of signals from very low to very high power levels in the presence of intentional and unintentional interfering signals," says Mark Faulkner, chief technologist, RF and Microwave Systems, at Mercury Systems in Los Angeles. "At the front end, what limits your dynamic range is typically the mixer; the higher the linearity of your mixer, the better. There's always folks working on that problem; it's one of the fundamental limitations to our systems. We have ways to get to 40 dBm [decibels per milliwatt], but at the cost of high LO [local oscillator] drive and DC power."

For example, says Faulkner, "Let's say in the [UAS], the RF has to process very high data rates – we're looking at several things going across the channel right now. You have to run real-time video from your [UAS], probably GPS data, potentially a [communications] link, telemetry, and the ability to redirect assets. All of this places demands

on the data rates and the RF links. You have to actually design systems that can handle that new capacity."

Interestingly enough, the UAS challenges of the near future "may not be so much on the analog side, directly," D'Arcy says. "What I see as the biggest challenge, and what I deal with a lot, is what to do with all the data that we can either pull out of, or put into, the analog side of the signal chain. We are at risk of over-driving the digital side."

Digital domain

The overload of information that a UAS needs to process has a direct effect on how these systems are being designed. In fact, some designers are saying that the RF content is not increasing: "My assessment is that RF content is decreasing," Faulkner says. "The reason I say that is because the digital domain is getting faster and faster. It's actually going to replace some of the RF functions, and it already has in some cases," Faulkner says. "A/D [analog-to-digital] converters are becoming so fast right now that we can already get rid of the second frequency conversion in our heterodyne dual-conversion downconverters. Just replace the second conversion with digital signal processing. We are moving these A/Ds closer to the antennae aperture as the speeds increase. I see that trend continuing."

The change comes in response to the increased load on the digital domain and the understanding that engineers need to take into account those digital constraints, D'Arcy says. "This will range from things like the JESD204 [serial-interface] standards to designs that may have to feed multiple paths and multiple points in the digital-processing chain. Historically, the people on the digital side and the programmers and the software engineers had to take exactly what was given to them from the analog side. Now we've become sophisticated enough that we can actually design the analog side with what the digital mission had in mind to begin with."

The emphasis on the digital side has pushed engineers to design differently. Along with new design methods come new challenges to solve. "Looking out as far as three years from now, because these A/Ds are now handling a lot of the RF and analog signal processing, it creates a bottleneck further downstream," Faulkner says. "If you have an AESA [active electronically-scanned array] radar on a [UAS], and now you have 100 low-power A/Ds, one behind each AESA element, you have to be able to process 100 individual 100 GSPS [gigasamples per second] lines with low latency. That's going to be the next challenge – more in the digital domain but it's driven by this trend of A/Ds moving closer to the aperture."

Electromagnetic spectrum

The digital side is not the only obstacle or design challenge within the UAS RF and microwave world. "There can be a lot of increased competition and interference across the RF and microwave spectrum, which could be radar applications or radios," D'Arcy says. "Primarily, we have some limitations in frequencies and frequency allocations," he adds. "There are some contentions in those spaces. There's a lot of geometry that is very specific to payloads and also some stabilization that's inherent in the airborne systems themselves."

For example, "You're using [UASs] to perform some long-endurance ISR that you may see in the military space," he explains. "You have a situation where you're trying to cover and monitor these large swaths of the spectrum. You're trying to pull out very specific signatures and profiles, both in real time and then in post-processing. This is becoming, as the use of the RF and microwave spectrum expands, an even more complex challenge. This occurs in the ISR space, not just in the military, but you're also starting to see this in law enforcement as well.

"Aside from things that you may communicate – along with the command and control of the beast itself or the bird itself – you're actually looking at how you send critical data back to the ground," D'Arcy says.

The different roles of UASs

The demand for unmanned systems to play different roles, whether military or civilian, has forced engineers to look at various aspects. These include modularity, which can mean that "the requirements often want to go through a respin without changing the base-level hardware," Faulkner says. "If you can make something modular and configurable, such that you can enhance its functionality later, maybe through software, that's another key challenge that we're facing these days."

Designers have to figure out where RF and microwave content belong in the UAS scheme, Parthasarathy says. "In the end, where is this going? If you look at it from the perspective of what unmanned systems eventually want us to do, I think there are several drivers. One is the whole idea of autonomy. The second one is manned and teaming. Think about words that are used, like swarming or man/unmanned teaming. The problem really is how to accomplish multiple missions – so the demands are similar to those of communications customers: a wider frequency range, more agility, directed links, and protected communications.

Figure 1 | The Analog Devices HMC 1099 power amp addresses range and power-consumption requirements. Photo courtesy of Analog Devices.

"On the surveillance side, of course radar is a big thing," he continues. "Both in the sense-and-avoid perspective to ensure safety and operations, especially operating in national airspace, but also from a perspective of sense in synthetic aperture radars (SARs) and imagery radars. What users are looking for in our technologies for surveillance is technology that enables us to span various bands. Finally, on the effects side, it's all about more autonomy, the sense of communications enablement."

Analog Devices' HMC 1099 power amplifier (Figure 1) addresses some of these challenges. "The HMC 1099 is a 10-watt, gallium-nitride (GaN) power amplifier, in about the one to 10 gigahertz range," D'Arcy explains. "It provides a wide instantaneous bandwidth, but also has a really low power consumption. It is designed for applications such as radio, communication systems, phased arrays. It could be either in the radar space or it could be in the phased antenna space." **MES**

Security plays a major role in RF realm

Department of Defense (DoD) officials are asking for additional security in all unmanned systems. "The industry is looking to do more encryption as close to the analog-to-digital converter or the digital-to-analog converter as you possibly can get," says Sean D'Arcy, strategic marketing, Aerospace and Defense, at Analog Devices in Chelmsford, Massachusetts.

The demand for security has a lot to do with communications: "We talk about a 'robust' or 'agile'-type frequency hopping, possibly jam-resistant technology. You could expect the encryption that goes with that probably to move down to a lower level," D'Arcy says. "Some of the RF frequency hopping would be allowed in the payload space, but also in the command-and-control space, of the [UAS] operations. You would really need to prevent any type of flyaway situations jamming, or possibly even takeover of a [UAS]. You can see very low-level but high-encryption security going forward."

For example, "If one of our [UAS] assets ends up behind enemy lines, we do not want them to be able to reverse-engineer it," says Mark Faulkner, chief technologist, RF and Microwave Systems, at Mercury Systems in Los Angeles. "There are techniques, including RF techniques, that you apply physically to the package itself to prevent exposure of our intellectual property. The packaging itself includes RF elements that are sensitive to tampering and can trigger sanitization routines. Another example would be how to process these RF streams such that they cannot be intercepted or hijacked. Or even if they are intercepted, how can we make them so robust that they cannot be altered? We don't want somebody else to take control of the UAS if they had their own control mechanisms."

SWaP and affordability is the DoD's mantra

Requirements for equipment across the board today are calling for smaller size, weight, and power (SWaP). Engineers are trying to get as much RF content in as small a volume as possible, says Mark Faulkner, chief technologist, RF and Microwave Systems, at Mercury Systems in Los Angeles. "One of the key requirements for unmanned systems is fitting as much spectral density in a small volume, with the lowest power consumption possible. That way they can fit more functionality within the [UASs]." One way to address the push for SWaP is to use "multilayer thin-film packages or reprogrammable field-programmable gate array (RFPGA) packages," Faulkner says. "Highly-integrated mimics that perform multiple functions or heterogeneous semiconductor integration get the best of both those semiconductors for their particular strengths."

What will all this innovation equate to? "Affordability, which seems to be the mantra for all we do, along with SWaP," explains Sanjay Parthasarathy, senior vice president of strategy at Cobham Advanced Electronic Solutions in Washington.

Hardening flash storage for ultimate data security

By C.C. Wu

Whole-drive data encryption now enables designers to build in robust data security for storage drives – even flash storage – intended for unmanned aerial systems (UASs), making surveillance and reconnaissance data more secure. The MQ-9 Reaper UAS is flown over the Southern California Logistics Airport in Victorville, California, by the 163rd Reconnaissance Wing. (Air National Guard photo/Senior Airman Michael Quiboloy)

Today's flash storage has made it possible to make embedded systems lighter, faster, more energy-efficient, and more compact than ever. With no moving parts, their reliability is unrivaled and they're the perfect storage medium for rugged applications. However, the nature of flash also makes it more difficult to erase data securely than with traditional magnetic storage. Modern wear-leveling algorithms designed to maximize drive life are extremely effective, but also make it difficult to encrypt files individually or ensure data is ever completely erased. All is not lost: Whole-drive encryption enables engineers to provide strong data security, even with modern flash drives. For military applications its benefits are clear, for both securing data as well as securely erasing sensitive data at the push of a button.

The Hainan Island incident

In 2001, a U.S. Navy EP-3E Aries II reconnaissance plane collided with a Chinese jet and was forced to land at a Chinese military airfield on Hainan Island. Its crew had only twenty minutes to destroy sensitive data before being ordered off the plane at gunpoint. They resorted to pouring hot coffee into hard disk drives and attacking electronics with axes.

This method was unfortunately insufficient. Data was still recoverable by Chinese computer experts and the event was a significant setback for U.S. intelligence, according to some accounts. In a separate incident a few years later, embarrassed U.S. officials learned from news media that flash drives taken from a military base in Afghanistan were not only being sold in a nearby bazaar, but also still contained secret files that named enemies targeted for kill or capture, and described efforts to remove uncooperative local officials.

Cybersecurity incidents like these show us just how challenging it is to lock down sensitive data – and how damaging it can be when security procedures fail. Military and intelligence professionals are becoming increasingly aware of the need for cyber hardening of information systems, on multiple levels, to protect them from any conceivable threat.

A solid foundation

Securing an embedded system starts with protecting the data itself, so even if an adversary gains access, they will still be stymied by a final, unbreakable bedrock layer of security. Two complementary ways exist for achieving this goal: encrypting the data and destroying the data.

A secure drive's first line of defense is encryption

The latest secure flash drives can protect all their data with an algorithm that is effectively unbreakable by any known or foreseeable technology: AES 256-bit. Accessing

the data on the drive requires two secure keys – effectively very long passwords.

One of the keys is generated by the drive itself, stored in a secure area inside the drive and never revealed to the outside world; the other key is known to the authorized user. The data can only be read with both keys. Attempting to guess the keys, by trying every possible combination, would take trillions of years.

In normal operation, the user's key is requested whenever the system with an encrypted SSD (solid-state drive, or flash drive) is powered on. Depending on the application, the drive could request re-authorization for other users or to access more sensitive data and operations, or on a timed basis.

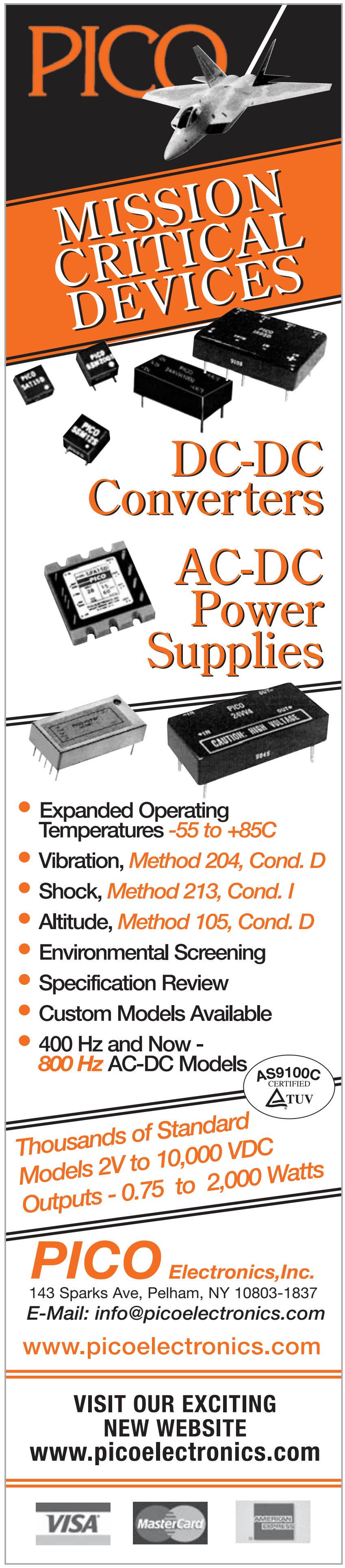
AES drives contain hardware that encrypts and decrypts all data in the background, as it is written to the disk, so there is no impact on drive performance. All data stored in the drive is always protected with unbreakable AES 256-bit encryption.

Data access on a "need-to-know" basis

AES drives are compliant with the TCG OPAL 2.0 standard, which allows multiple passwords or keys, each suited for different levels of security clearance and different modes of access to the data.

In a modern scenario, the crew of a reconnaissance aircraft similar to the U.S. EP-3E that was forced down in China might only have a password that permits their onboard sensors to write gathered intelligence data to a secure drive. During their mission, their sensors could freely write data to the drive, but the crew would not possess the password required to read that data back afterward.

The crew would therefore be physically incapable of revealing the data to an enemy. In addition, the drive's AES 256-bit encryption would prevent enemy access, even if the plane was captured intact. The data can only be read when the aircraft returns safely to base, by personnel with a higher-level password which is not in the possession of the crew on board.



Last resort – erase or destroy

Being able to securely erase or destroy physical data on a drive provides the final layer of defense for a truly robust military information system. If an asset falls into hostile hands, or an adversary gains access by some other means, timely destruction of the data can still frustrate all their efforts and leave them holding a useless piece of hardware that no longer has any secrets to give up.

Self-encrypting drives with built-in mass data-deletion capability also bring more mundane benefits. Most notably, they expedite easy disposal or reallocation of storage media as part of normal operations. A robust data-sanitization policy helps prevent accidental leaks of sensitive data, including personal data covered by national data-protection laws.

Various modes of emergency data deletion can be used separately or together depending on operational requirements, in accordance with the end user's organizational standards and government regulations.

Initiating a drive erase operation in the field

Emergency drive erase operations can be done either directly through physical action, or remotely. Of course, removing the drive from its enclosure and moving a tiny jumper onto the erase pins is not an appropriate task for a combat or emergency situation – that could take many minutes and require care and manual dexterity. Therefore, a real-world implementation will typically link the erase pins to a more easily-accessible external control. This should be shielded from accidental activation, and perhaps require a key, dual operators, or multiple steps to activate.

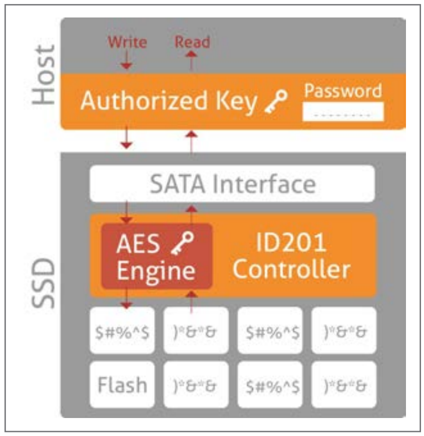


Figure 1 | Drives with AES self-encryption, such as the Innodisk 3MG2-P, use a hardware encryption engine to secure data transparently, without affecting drive performance.

Remote erase

Military and intelligence operations are increasingly looking at replacing reconnaissance aircraft, like the U.S. Navy EP-3E involved in the Hainan incident, with remotely-operated drones. While this helps keep valuable personnel out of harm's way, it perhaps makes data even more vulnerable.

Consider a scenario when a drive full of sensitive data is onboard a drone that is going down over enemy territory. Physical access to the erase jumper pins is impossible. The alternate method of activating erase functions is remotely, via a command sent over the drive's interface from the controlling computer. Although this course of action might heighten concerns about accidental or malicious activation, good, secure systems design can mitigate these. The built-in ability for a remote erase also makes a programmed erase function possible. For example, a drone could be programmed to wipe its data if it loses contact with its base, or if an unauthorized attempt at physical access is detected.

Multiple data-deletion methods

Innodisk's data-deletion technologies comprise quick-erase, security erase, and destroy functions. With quick erase, an internal flash-erase command is sent and the data on the flash memory is deleted. Due to concerns that residual data may be left on the drive, a more stringent erase function, called security erase, can be used. Security erase deletes the data by following a more complex series of steps, including erasing and physically overwriting, and possible repetition of these steps. (Figure 1.)

There exist a number of security erase processes, most of which are devised by the U.S. military and intelligence services. The Innodisk drives support many of the standards; the user is able to select the particular standard used.

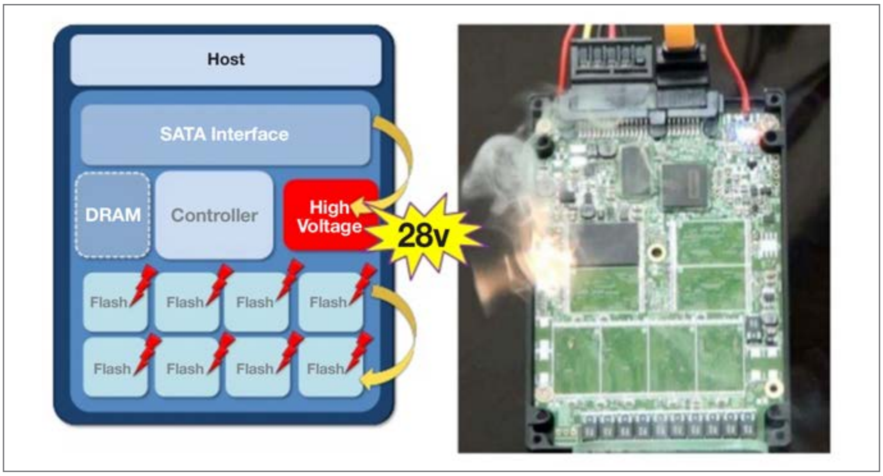


Figure 2 | Using high voltage to completely destroy flash cells and firmware, the physical destroy function makes data completely and irreversibly unrecoverable.

> VARIOUS MODES OF EMERGENCY DATA DELETION CAN BE USED SEPARATELY OR TOGETHER DEPENDING ON OPERATIONAL REQUIREMENTS, IN ACCORDANCE WITH THE END USER'S ORGANIZATIONAL STANDARDS AND GOVERNMENT REGULATIONS.

Emergency data deletion

Looking at the time required for various erase modes, quick erase is by far the fastest, typically requiring around five to 10 seconds, depending on disk size and write speed. Security erase requires minutes, or sometimes hours, to completely erase all data. However, because the first step of almost all security erase standards is effectively a quick erase operation, the slower speed of security erase would not seem to add any additional security hazard in those cases.

The "destroy" function is a proprietary process that effectively makes all data unrecoverable, including the firmware, which controls the drive. This function is a physical self-destruct process, which deliberately exceeds every flash chip's voltage specifications to destroy the hardware. (Figure 2.) The destroy operation is irreversible: Not only is the data made inaccessible, but the drive cannot be repaired and made functional again.

Ultimate data security

When we consider the cases of military data breaches such as those in China and Afghanistan discussed earlier, we can see how new security technologies can keep data secure if such incidents occur today. One-button erase technologies built into flash drives enable a busy, combat-stressed crew to quickly erase sensitive data. If or when drives fall intact into hostile hands, encryption can still make the drives unreadable for even the most skilled and determined adversary. **MES**

C.C. Wu is vice president of Innodisk and director of the Embedded Flash division. He is a frequent presenter at the annual Flash Memory Summit held in Santa Clara, California, and speaks on the topics of NAND flash technology and embedded systems storage.

Innodisk • www.innodisk.com

Optimizing your video-enabled drone design

By Dennis Barrett

Low-latency video transmission is a key component of safe drone or unmanned aerial system (UAS) operation, both military and civilian. U.S. Army photo/Photo credit: David Vergun.

The global aerial drone/unmanned aircraft market could be worth $127 billion by 2020, up from just $2 billion today, according to a market report from consulting firm PWC. To better understand the safe operation of drones, let's dive into a key requirement for enabling safe flight: low-latency video transmission.

To operate outside of a user's line of sight, any drone needs to feature an onboard camera with real-time transmission capabilities. When selecting the right system for the job, it is important to keep these factors in mind:

- Low power consumption: Lower power increases flight times
- Low latency: Lower latency enables faster reactions
- Wireless link robustness: Robust connections increase accuracy and responsiveness
- Range: Longer range extends distance of operation
- Autonomy: Additional sensors enable safer flights

Of these considerations, low-latency video compression and transmission is of the utmost importance. The following methods outline several ways developers can reduce latency to a drone's video compression and transmission system:

- Video capture: A higher frame rate means lower capture times (T_{cap}). For example, a 30-fps camera takes 33 ms to capture each frame of video. This number is reduced to 16.5 ms for 60-fps video capture.
- Compression or encoding: Compression techniques are used to reduce the data rate needed for transmitting video frames. The H.264 compression standard is a very common technique for recording and compressing video in drones. Compression is generally a compute-intensive task. The time required to encode (T_{enc}) depends on the choice of encoding engine and features used.
- Transmission: Drones communicate to the ground station using a wireless communication mechanism like Wi-Fi connectivity. The resulting transmission delay (T_{tx}) depends on the available data bandwidth. For example, if a 720p30 stream is encoded at 1 Mbps and the available bandwidth is 2 Mbps, the time taken to send a stream to the ground station is 16.5 ms.
- Network: Depending on the need, an aerial system may be connected to remote ground stations via a network. If this is the case, additional delays (T_{nw}) may result within the network.
- Receive: If the ground station is also wirelessly connected to the network, then additional latency (T_{rx}) similar to that of transmission is involved in the system.
- Decompression or decoding: The compressed video stream needs to be decompressed at the receiving station. Like encoding, this decoding process is also compute-intensive, introducing a decoding delay (T_{dec}) to the system.
- Display: Just like video capture, there will be display latency (T_{disp}) depending on the refresh rate.

One thing to also note is that a drone communicating directly with ground stations does not need to rely on a network, resulting only in a single transmission delay (T_{tx}) (i.e., $T_{nw} = 0$ and $T_{rc} = 0$).

To better illustrate the total latency from capture to display during frame-by-frame operations, Figure 1 details a timeline of this process.

A specific example of total latency may be found in Table 1.

Outlined in Table 1 is a high-latency scenario for controlling drone operations. Here it takes 118.7 ms for the operator to see the collected video. If a drone is traveling at 15 meters per second, it will have moved 1.8 meters when the remote operator sees the need for a flight change; during this time the drone could crash.

To help reduce this possibility, the H.264 standard introduces the concept of slices. A slice is composed of several macroblocks (a two-dimensional unit of a video frame), which are encoded independently. Using this approach enables each slice to be decoded separately without referencing another. However, while low-latency encoding offers flexibility in how to arrange these slices, using the natural row order is most efficient.

When the number of slices in a frame is greater than one, developers have the ability to reduce not only encoding time but also overall latency. In this situation, the system only has to wait for one frame to be captured before encoding begins, automatically triggering its transmission. The impact is that the capture, encode, transmission, receive, decode and display process is no longer serial but parallelized, introducing a theoretical reduction of delay by a factor of N at each step. This makes the overall latency: $T = T_{cap} + (T_{enc} + T_{tx} + T_{nw} + T_{rx} + T_{dec} + T_{disp})/N$ (Figure 2).

In theory, the effective time will be reduced by a factor of N between the encode and display processes. However,

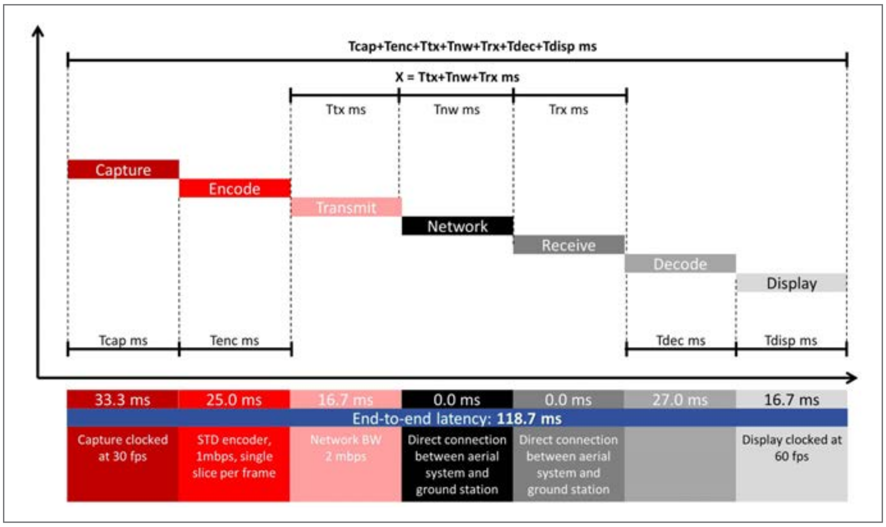


Figure 1 | Video capture and display timeline.

System blocks	Latency in ms	Comments
T_{cap}	33.3	Capture clocked at 30 fps
T_{enc}	25	STD encoder, 1 Mbps, single slice per frame
T_{tx}	16.7	Network bandwidth 2 Mbps
T_{nw}	0.0	Direct connection between aerial system and ground station
T_{rx}	0.0	Direct connection between aerial system and ground station
T_{dec}	27	
T_{disp}	16.7	Display clocked at 60 fps
End-to-end latency	118.7	Assume zero network latency

Table 1 | Frame-by-frame latency example.

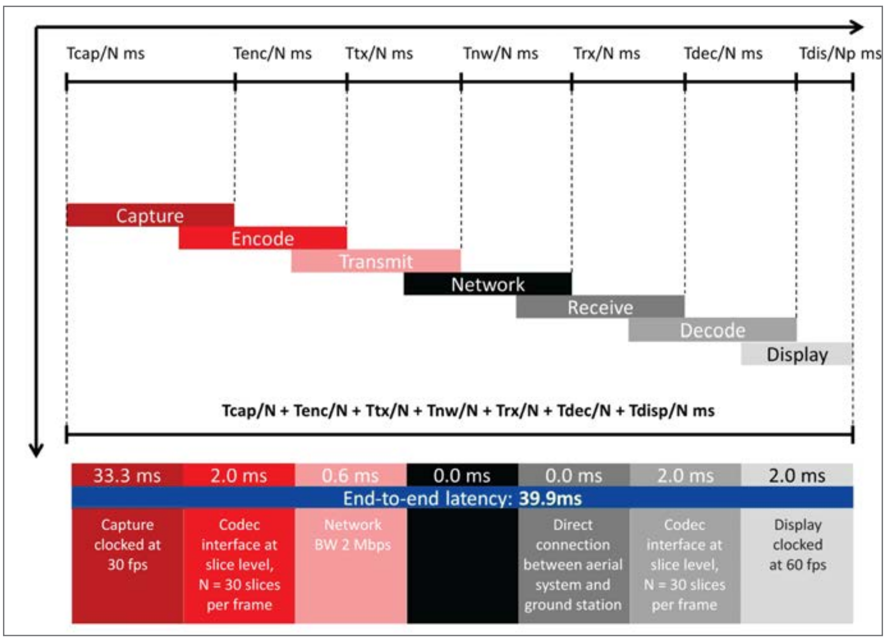


Figure 2 | Slice-based impact on processing timeline.

practically, the time may not always scale linearly with the number of slices, an effect caused by the overhead required to set up and process individual slices. Table 2 shows sample latency for slice-based encoding based on a rate of 30 slices per frame.

As in this example, even if an effective encoding/decoding time is achieved, the latency still takes half the time of frame-based encoding (single slice per frame). By using this process, the remote drone pilot is able to react at least three times faster.

One tradeoff to consider: While a higher number of slices will speed up the encoding and transmission process, it also reduces the compression ratio. This method increases the number of bits used for a slice along with the effective transmission time. The designer must optimize the end-to-end system; ultimately, it will be up to them adjust this parameter accordingly.

System blocks	Latency in ms	Comments
T_{cap}	33.3	Capture clocked at 30 fps
Effective T_{enc}	2	Codec interface at slice level, N = 30 slices per frame
Effective T_{tx}	0.6	Network bandwidth 2 Mbps
T_{rx}	0.0	Direct connection between aerial system and ground station
Effective T_{dec}	2	Codec interface at slice level, N = 30 slices per frame
Effective T_{disp}	2.0	Display clocked at 60 fps
End-to-end latency	39.9	

Table 2 | Slice-based latency example.

Digital media processors leverage integrated hardware engines along with frame-to-memory ISPs designed for the low-latency encoding and decoding of videos, using multiple slices per frame. Figure 3 shows a drone's digital media processor in a low-latency video-encoding Wi-Fi system.

Wi-Fi and Bluetooth combo-connectivity devices are equipped with advanced features required for drones, such as antenna diversity, maximal ratio combining, dual-band support (2.4- and 5-GHz bands), rate management, and optimized data path.

If onboard monitoring of the aerial system is desired, using the UART interface exchanges control data with the drone's central control unit, which enables autonomous collision avoidance.

Drones represent an exciting technology platform for engineers that are constrained by most design variables like the size, weight, power, and cost [SWaP-C]. Controlled flight – a challenge unchanged since the time of the Wright brothers – requires low-latency video processing, whether delivery is over a wireless connection for the operator or ultimately fully autonomous operation. By employing slice-based processing of the full video frame and streaming multiple channels of compressed video, designers will be able to provide flexible, ultra-low-latency video delivery for drone flight. **MES**

References

1. Marcelo Balve, Business Insider, 13 Oct 2014 – Commercial Drones: Assessing the Potential for a New Drone-Powered Economy – www.businessinsider.com/the-market-forcommercial-drones-2014-2
2. PwC May 2016 – Clarity from above – PwC global report on the commercial applications of drone technology – www.pwc.pl/clarityfromabove

Dennis Barrett *is a Product Marketing Engineer, Video and Vision Analytics, at Texas Instruments. He has worked on DSP, processor, and controller solutions for 30 years.*

Texas Instruments
www.ti.com

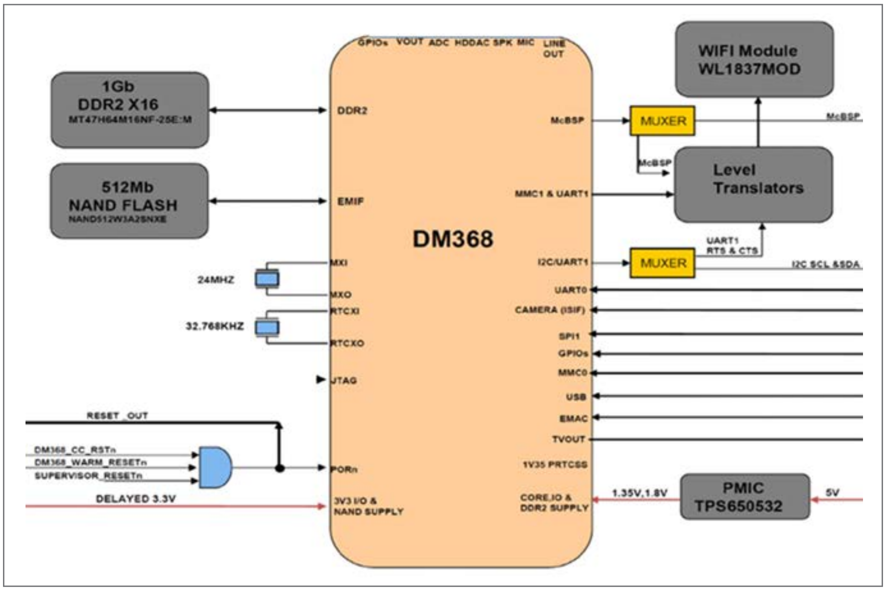
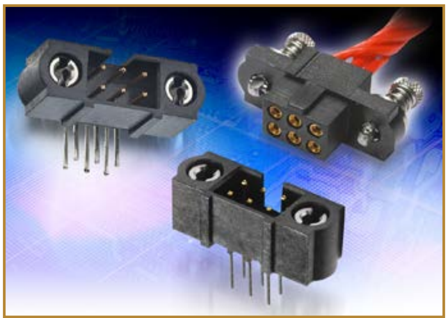


Figure 3 | The TMS320DM368 digital media processor in a low-latency video-encoding Wi-Fi system for use in drones.



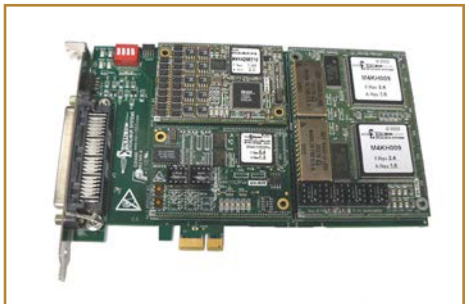
Harwin's Datamate 2-mm jackscrew connectors for high-reliability industries

Harwin's Datamate jackscrew connectors, aimed at high-reliability applications, come in a variety of connector systems with a choice of slotted or hex socket jackscrew fixings, with board mount for PCB connectors. The pole connectors are marked with "#1 contact" and are available in single-, double-, and triple-row configurations. According to the company, industrial applications such as satellites, robotics, and motor sports now prefer to specify high-reliability connectors with jackscrews, rather than latches or other fixing mechanisms, to ensure a secure connection. The J-Tek jackscrew fixing is also being used in different industries to connect printed circuit boards (PCBs) together in configurations where space is at a premium.

Satellites, especially miniature CubeSats, use jackscrews not only to ensure that the connection survives harsh operating conditions, but also to save space. Harwin recommends that users torque Datamate jackscrews to 21 +/- 2 cN/m. This tightness ensures that devices meet EIA specifications for vibration severity. Jackscrews are available with all Harwin's Datamate and Mix-Tek (mixed signal, power, and coax) connectors. Features of the Datamate family include 3A per signal contact, 500 mating cycles durability, four-finger contact design to maintain electrical contact through high vibration and shock, and beryllium copper contact for extended temperature range: -55 °C to +125 °C (testing in progress to confirm higher).

Harwin | www.harwin.com | www.mil-embedded.com/p374120

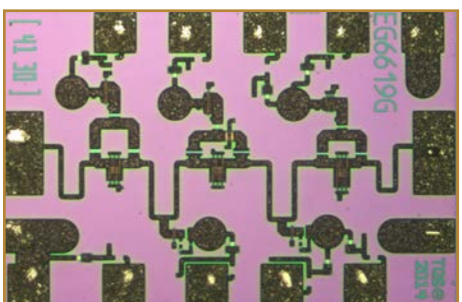
Multiprotocol interface for PCI Express-compatible systems



The EXC-4000PCIe/xx is a multiprotocol interface for PCI Express-compatible systems. Excalibur Systems intended the card for the PCI Express bus; it supports as many as four dual-redundant 1553 channels using the M4K1553Px(S) module. The EXC-4000PCIe/xx interface is compatible with all common variations of MIL-STD-1553A and B and can be either multifunction or single-function.

Under the multifunction mode of the EXC-4000PCIe/xx, each channel using the M4K1553Px module operates simultaneously as a bus controller and/or multiple (as many as 32) remote terminals, or as a triggerable bus monitor. In addition, error injection (BC and RT modes) and error detection (all modes) are supported on each channel. In the single function, each channel using the M4K1553PxS (RT validated) module operates either as a bus controller, remote terminal, or bus monitor. The EXC-4000PCIe/xx is supplied with C drivers (including source code) and Merlin+ Windows software and may be used with Exalt, Excalibur's Analysis and Laboratory Tools, a Windows monitoring application. A mating connector is provided for I/O connection.

Excalibur Systems | www.mil-1553.com | www.mil-embedded.com/p374056

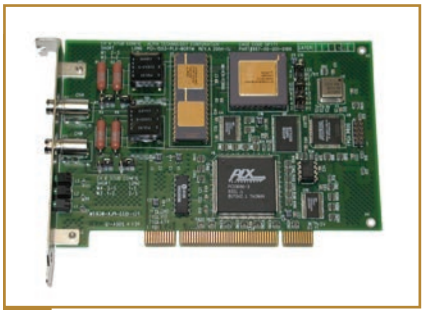


Wideband digital attenuator offers low LSB of .5 dB

Qorvo's TGL2223 is a wideband, 5-bit digital attenuator using the company's TQPHT15 production 0.15um GaAs pHEMT process. Operating from 0.1 - 31 GHz, the TGL2223 offers a low attenuation step size (LSB) of 0.5 dB and supports > 15.5 dB of attenuation range with a low RMS step error of < 0.5 dB. Using standard, negative control voltages from -3.3 to -5 V coupled with broadband performance, the TGA2223 is aimed at a variety of commercial and military applications.

The TGL2223 is in die form, measuring 1.180 by 0.800 by 0.100 mm, with both radio frequency (RF) ports matched to 50 ohms for simple system integration. It is lead-free and RoHS-compliant, with evaluation boards available on request. The frequency ranges between 0.1 to 31 GHz. Features also include insertion loss (Ref. State): 1.8-4.2 dB; RMS Step Error: < 0.4 dB; and control voltage ranges between -3.3 to -5.0 V. Typical applications include commercial and military radar, electronic warfare, point-to-point radio, and satellite communications.

Qorvo | www.qorvo.com | www.mil-embedded.com/p374128



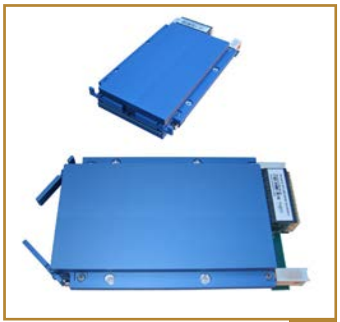
PCI-1553-PLX offers option for UTMC's Sμmmit or BCRTM communication device

The PCI-1553-PLX module from ALPHI Technology Corp. uses a single UTMC's Sμmmit or BCRTM communication device as its 1553 bus controller, remote terminal, or monitor terminal. The single controller has two redundant channels; this controller accesses 64K by 16 words of external memory and has externals for both channel A and B. The 3U PCI board has onboard transformers for both channels, which enables the use of a wide array of 1553 communication applications including test equipment supporting evaluation, simulation, monitoring, and analysis; operational equipment such as avionics, space satellite systems, aircraft onboard systems, and commercial systems; and applications that require dual functionality of the terminal for monitoring and remote operation at the same time.

Features include one controller of dual-redundant (A/B channel) 1553 communications; UTMC's BCRTM or Summit controller options; programmable bus controller, remote terminal, or monitor terminal modes; MIL-STD-1553 A and B compliance, Notice 2 RT; long or short stub support; low power consumption; PICMG compliance; +3.3V or +5 VDC VIO; LED status notice; and selectable external or internal clock.

ALPHI Technology Corp. | www.alphitech.com | www.mil-embedded.com/p374122

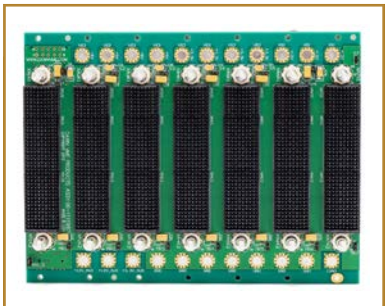
3U VPX storage module with REDI conduction and air-cooled configurations



Phoenix International's VP1-250-SSD/HDD [solid-state drive/hard disk drive] Serial ATA (SATA)-based VPX blade delivers high capacity data storage for military, aerospace, and industrial applications requiring rugged, secure, and durable mass data storage. The VP1-250-SSD/HDD is a 3U VPX storage module that can support either a rotating or solid-state hard drive. When used with supporting media, the VP1-250-SSD/HDD supports the "purge" input signal to destroy the media or the "zeroize" command that performs a Department of Defense (DoD)-approved erasure of the media in case of hostile seizure.

The VP1-250-SSD/HDD provides high transfer and I/O rates, enhanced endurance, and maximum data integrity. Features include REDI conduction and air-cooled configurations; it supports SATA and PCI Express interfaces and can operate at up to 80,000 feet of altitude. The temperature range extends from -40 °C to +85 °C. Users can connect the module as a SATA drive or via the PCIe interface. It also features a jumper-selectable SSD of up to 4 TB and can feature rotating disk drives (RDDs) as many as 4 TB. It can be configured to work from fat pipe A or B from the VPX bus, can perform as many as 80,000+ 4 KB random IOPS [input/output operations per second], and uses integrated single-level cell (SLC), multilevel cell (MLC), enterprise MLC (eMLC), or NAND SSDs. The VP1 meets military and IRIG telemetry 106•07 declassification standards.

Phoenix International | www.phenxint.com | www.mil-embedded.com/p374123



OpenVPX backplane for signal integrity at up to 10.3 Gbaud

Dawn VME's VPX-5987 backplane is designed to deliver robust signal integrity at Gen3 bandwidths. The backplanes are designed for signal integrity at up to 10.3 Gbaud performance (per VITA 68 backplane simulation models). Supporting PCIe Gen3 and 10 GbE (XAUI) and the most recent Gen3 bandwidth module configurations, Dawn Gen3 backplanes offer multiple connector choices, including a high-vibration option.

Features include 7-Slot – BKP3-CEN07 (6 Payload + 1 Switch); 3U OpenVPX-compliant, 1-inch pitch; various connector choices; and use of any desired power supply for the terminal block and bus bars. The 598x Series VPX backplanes are also designed to be compliant with the following released standards and December 2015 state of draft specifications: VITA 46.0, VITA 46.1, VITA 46.3, VITA 46.4, VITA 46.6, VITA 46.7, VITA 46.9, VITA 46.10, VITA 46.11, VITA 48.0 (REDI), VITA 48.1 (REDI Air Cooling), Vita 48.2 (REDI Conduction Cooling), and VITA 65.0 (OpenVPX) ready. VITA 68 backplane models are available on request for system simulation.

Dawn VME Products, Inc. | www.dawnvme.com | www.mil-embedded.com/p374124

Mimicking birds' flight could be the next step in drone design

By Mariana Iriarte, Associate Editor

Stanford University researchers are taking a closer look at the way animals fly, more specifically at the circular patterns of rotating air or vortices created by birds. The results of this study, it is hoped, will lead researchers and engineers to design drones that can better navigate in obstacle-filled areas.

The Office of Naval Research (ONR) is sponsoring the Stanford research project, with additional funding from the KACST-Stanford Center of Excellence for Aeronautics and Astronautics, a National Defense Science and Engineering Graduate Fellowship, and a Stanford Graduate Fellowship under ONR's Multidisciplinary University Research Initiative (MURI).

The goal of a program like MURI is to investigate Department of Defense (DoD) topics that will one day help the military.

The flight-focused study with Stanford University focuses on unmanned and autonomous flight. Dr. David Lentink, Stanford assistant professor of mechanical engineering, is leading a team that found inaccuracies in the current ways of measuring vortices that birds create when they fly. Accurate measurements in this area is important for drone design because studying the way in which birds produce enough lift to fly will enable researchers to learn how to better create robotic wings, ultimately giving a drone more flexibility.

In an ONR release, Lentink explains: "For a long time, engineers have looked to animal flight literature to see how robotic wings could be designed better. But that knowledge was based on inaccurate models for lift. We now know we need new studies and methods to inform this design process better. I believe our method, which measures lift force directly, can contribute to such improvements."

The results – published in the December 2016 issue of Bioinspiration & Biomimetics titled "Lift calculations based on accepted wake models for animal flight are inconsistent and sensitive to vortex dynamics" by Eric Gutierrez, Daniel B. Quinn, Diana D. Chin, and David Lentink – showed that much more research is still needed.

Lentink and his team trained a Pacific parrotlet named Obie to fly from perch to perch through a laser field infused with microparticles (see Figure 1). No animals were harmed in the experiment, as Obie wore laser safety goggles during each flight.

The team used three methods for calculating the lift. They found, however, "The three models predict different aerodynamic force values mid-downstroke compared to independent direct measurements with an aerodynamic force platform that we had available for the same species flying over a similar distance," as Lentink points out in his paper. In scientific research, the same repeated outcome is what really matters to prove a theory. "The researchers then applied each of the three prevailing models to these new measurements multiple times. In each case, the existing models failed to forecast the actual lift of the parrotlets."

Obie and several other parrotlet friends flew several times through the laser minefield, with nontoxic aerosol particles lighting up their path. Marc Steinberg, ONR program manager, says of the experiment, "One of the most exciting recent advances in understanding flying animals has been the use of new technologies like this to collect all kinds of data in free-flight conditions." Steinberg, who oversees the ONR/Stanford research, states in the release: "We can learn what's really happening – the biology and physics – and apply it to create UAVs [unmanned aerial vehicles] capable of navigating challenging

Figure 1 | Obie the parrotlet wearing goggles before flight through a laser field. Image courtesy of Stanford University/Eric Gutierrez.

environments like under a thick forest canopy or through urban canyons."

High-speed cameras captured the birds' wing tips and thus created a picture of the vortices. The data was combined with an aerodynamic force platform (a Lentink Lab instrument that was created with ONR's support).

"The platform is basically an ultrasensitive weight scale that measures the force generated when a bird takes off in a specially designed flight chamber," says Lentink. This measurement technique was developed by Lentink and his team; direct force measurements are used with flow measurements to create a more accurate model of aerodynamic phenomena in animal flight.

Going forward, Stanford University and ONR will continue the flight study. Their goal: Applying the information they have obtained toward how drones and UAVs can complete missions in hard-to-navigate areas. In such situations, the much-needed flexibility of Mother Nature's wings could be especially useful.

Lockheed Martin continues fighting cybercrime for DoD

By Sally Cole, Senior Editor

A recently won $347 million contract enables Lockheed Martin to continue overseeing the world's largest accredited digital forensics lab for five more years, as the company continues its role as the prime contractor for the Department of Defense (DoD) Defense Cyber Crime Center (DC3). Operating under the Air Force Office of Special Investigations, DC3's scope encompasses the entire DoD, providing operations, management, and mission support to more than 10 agencies, including the Department of Homeland Security (DHS), National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Defense Security Service (DSS), and U.S. Cyber Command (USCYBERCOM).

DC3's objective: To determine what adversaries are doing to copy, clone, steal, or destroy sensitive military and industrial secrets to gain a competitive advantage or an advantage in a warfighting scenario. "Our highly skilled cyber forensic analysts support this mission," says Tom Warner, program director for Lockheed Martin's DoD Cyber Solutions Division.

To this end, DC3's Defense Computer Forensics Laboratory (DCFL) receives "inputs from the defense criminal investigative organizations like the Air Force Office of Special Investigations, NCIS, etc.," Warner explains. "When digital assets – laptops, cellphones, etc. – are seized as part of crime investigations, they come to DC3. Our analysts do forensics examinations and pull together reports to be used in court to support the legal process."

Their capabilities include determining cyberattack attributions in order to gain a better understanding of adversaries and their infrastructure. "Analysts work to understand all of the details around specific cyberattacks and can provide that information to the appropriate authorities – law enforcement, counterintelligence, or the military – to help them perform their missions," he adds.

Another group within DC3, called RDT&E [Research, Development, Test, & Evaluation], specializes in development, tools, and support. "Our software engineers work in partnership with the government to develop capabilities that fill the gaps that COTS [commercial off-the-shelf] solutions can't accomplish today to help our employees find evidence on devices and do the analytics to better understand our adversaries from a cyber perspective," Warner says. But another central focus is "making cyber information-sharing easy" to help defend the defense industrial base and the DoD.

Nation-state cyberattacks on the DoD are escalating in terms of complexity, frequency, and stealth. These attackers are extremely well funded and resourced, and have a very clear directive on their objectives, unlike the noisy and relatively easy types of attacks that fraudsters and hacktivists tend to favor.

"Nation-state attacks – from our biggest adversaries – are the most challenging," Warner acknowledges. "They're driving us to innovate in the ways we defend against threats."

How do nation-state attacks get started? Most begin with social engineering and a targeted phishing email with a link to a compromised website to click as bait, where malicious code is waiting to be surreptitiously downloaded onto the victim's computer.

As Warner acknowledges, humans are the main reason DC3 exists. In many cases, he notes, "human action is what causes the initial compromise, and it's why we need to explore and understand how the initial compromise happened. Humans are one of our greatest assets, but also the biggest risk if they aren't educated to know how to handle these situations when they arise – report any suspicious emails and don't click links."

Nation-state attacks most frequently arrive in the form of what the Center calls advanced persistent threats, which are akin to "attempting to find a needle in a 'needlestack' rather than a needle in a haystack," Warner says. "These are well-resourced and trained adversaries who conduct multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national-security information."

Don't expect advanced persistent threats to go away any time soon. "The threat and ops tempo is increasing, stealth is ever-present, and these operations are downright surgical in terms of specific technologies they're targeting," Warner points out. "But as encryption becomes the norm, it's making it more difficult to understand the traffic that's potentially leaving networks – in terms of command and control between the adversary and the malicious code they have running on somebody's computers. This makes it more challenging to do investigations."

It's important to note that the threat is evolving as more devices become connected. Anything with an IP address is vulnerable and "there's a potential to connect in a malicious way," he adds. "Our data is everywhere – on smartwatches, phones, gaming, the Internet of Things, anything that's connected. A surprising amount of data resides on those devices. As our defense as a nation increases, our adversaries are continuing to evolve their attacks. We're doing our best to continue to keep ahead of that threat."

DC3 is one of Lockheed Martin's flagship cyber programs, and "we're thrilled to have the opportunity to support it for another five years," Warner says. For more on DC3, visit www.dc3.mil.

CONNECTING WITH MIL EMBEDDED

By Mil-Embedded.com Editorial Staff

CHARITY

Soldiers' Angels

Each issue in this section, the editorial staff of Military Embedded Systems will highlight a different charity that benefits military veterans and their families. We are honored to cover the technology that protects those who protect us every day. To back that up, our parent company – OpenSystems Media – will make a donation to every charity we showcase on this page.

This issue we are highlighting Soldiers' Angels, a national 501(c)(3) nonprofit organization that provides assistance and programs to aid the men and women serving in the United States Army, Marines, Navy, Air Force, and Coast Guard; deployed service members' families; and the growing population of veterans.

Soldiers' Angels was founded in 2003 by Patti Patton-Bader, the mother of a deployed Army staff sergeant. She began by simply sending care packages to her son in Iraq; the effort grew to include sending packages to his entire platoon.

Over the years the organization expanded its mission, with thousands of volunteers around the country involved in assembling tens of thousands of aid backpacks to Combat Support Hospitals, providing more than 6,000 computer devices with voice recognition for soldiers with wounds to their eyes and/or hands, shipping Kevlar blankets to protect unarmored Humvees in war zones, and setting up flights for families to reunite with their wounded troops. The nonprofit organization also runs the "Women of Valor" program, which honors female caregivers of post-9/11 wounded, ill, and injured service members.

In addition, the nonprofit is approved to work with the U.S. Department of Veterans Affairs Medical Centers, and offers resources, support, and remembrances to families whose loved ones have died in service to their country.

For more information, visit soldiersangels.org.

E-CAST

Unmanned aircraft and safety certification

Sponsored by Adacore, Curtiss-Wright, LDRA, and National Instruments

Autonomous aircraft, from small unmanned aerial vehicles (UAVs) to high-flying jet-powered platforms, are nearing certification to fly in multiple sections of the national airspace. Safety-related hurdles remain, such as properly certifying hardware and software for flight and convincing the public as well as commercial pilots that these craft are safe. Compliance with FAA safety standards such as DO-178 B and C for flight-critical software and DO-254 for hardware is moving forward.

In this e-cast, a panel of industry experts discuss the challenges that remain as well as solutions that will enable safe use of unmanned aircraft in civilian airspace and inspire confidence in the flying public.

View archived e-cast: ecast.opensystemsmedia.com/724

View more e-casts:
http://opensystemsmedia.com/events/e-cast/schedule

WHITE PAPER

Defense mission success with rugged SWaP-optimized Cobalt

By Kontron

Hughes Defense and Intelligence Systems (DISD) designed its HM200 Modem with specialized waveform enhancements for secure beyond-line-of-sight (BLoS) connectivity and high-speed data transfers even when transmitting through a military helicopter's rotating blades.

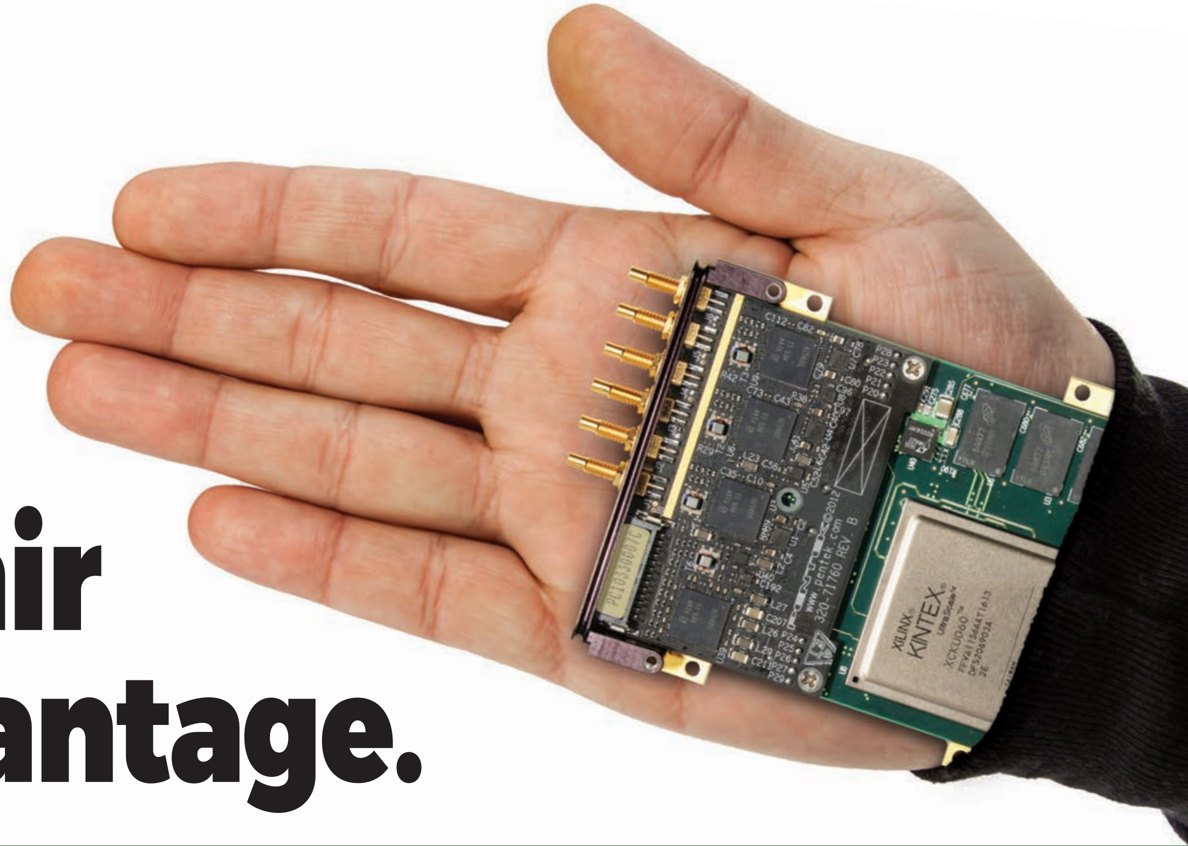
In this white paper, read how Hughes determined that the Kontron Cobalt platform could be used in its modem to meet the requirements for a rugged platform used in harsh environments.

Read the white paper:
http://mil-embedded.com/white-papers/white-success-rugged-swap-optimized-cobalttm/

Read more white papers:
http://whitepapers.opensystemsmedia.com


THE INTELLIGENCE
TO BE BETTER

Unfair Advantage.



2X HIGHER performance | 4X FASTER development

Introducing Jade™ architecture and Navigator™ Design Suite, the next evolutionary standards in digital signal processing.

Pentek's new Jade architecture, based on the latest generation Xilinx® Kintex® Ultrascale™ FPGA, doubles the performance levels of previous products. Plus, Pentek's next generation Navigator FPGA Design Kit and BSP tool suite unleashes these resources to speed IP development and optimize applications.

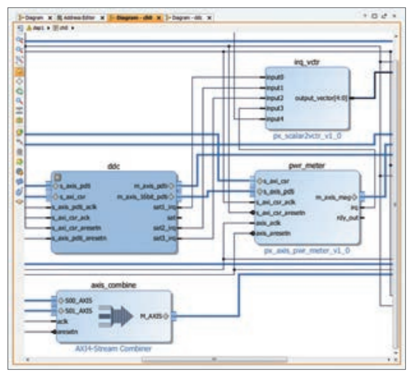
- **Streamlined Jade architecture** boosts performance, reduces power and lowers cost
- **Superior analog and digital I/O** handle multi-channel wideband signals with highest dynamic range
- **Built-in IP functions** for DDCs, DUCs, triggering, synchronization, DMA engines and more
- **Board resources** include PCIe Gen3 x8 interface, sample clock synthesizer and 5 GB DDR4 SDRAM
- **Navigator Design Suite** BSP and FPGA Design Kit (FDK) for Xilinx Vivado® IP Integrator expedite development
- **Applications** include wideband phased array systems, communications transceivers, radar transponders, SIGINT and ELINT monitoring and EW countermeasures

All this plus FREE lifetime applications support!

Jade Model 71861 XMC module, also available in VPX, PCIe, cPCI and AMC with rugged options.

JADE

Kintex Ultrascale FPGA



Navigator FDK shown in IP Integrator.

NAVIGATOR Design Suite

See the Video!
www.pentek.com/go/mesjade or call 201-818-5900 for more information

PENTEK
Setting the Standard for Digital Signal Processing

30 YEARS

Pentek, Inc., One Park Way, Upper Saddle River, NJ 07458
Phone: 201-818-5900 • Fax: 201-818-5904 • email: info@pentek.com • **www.pentek.com**